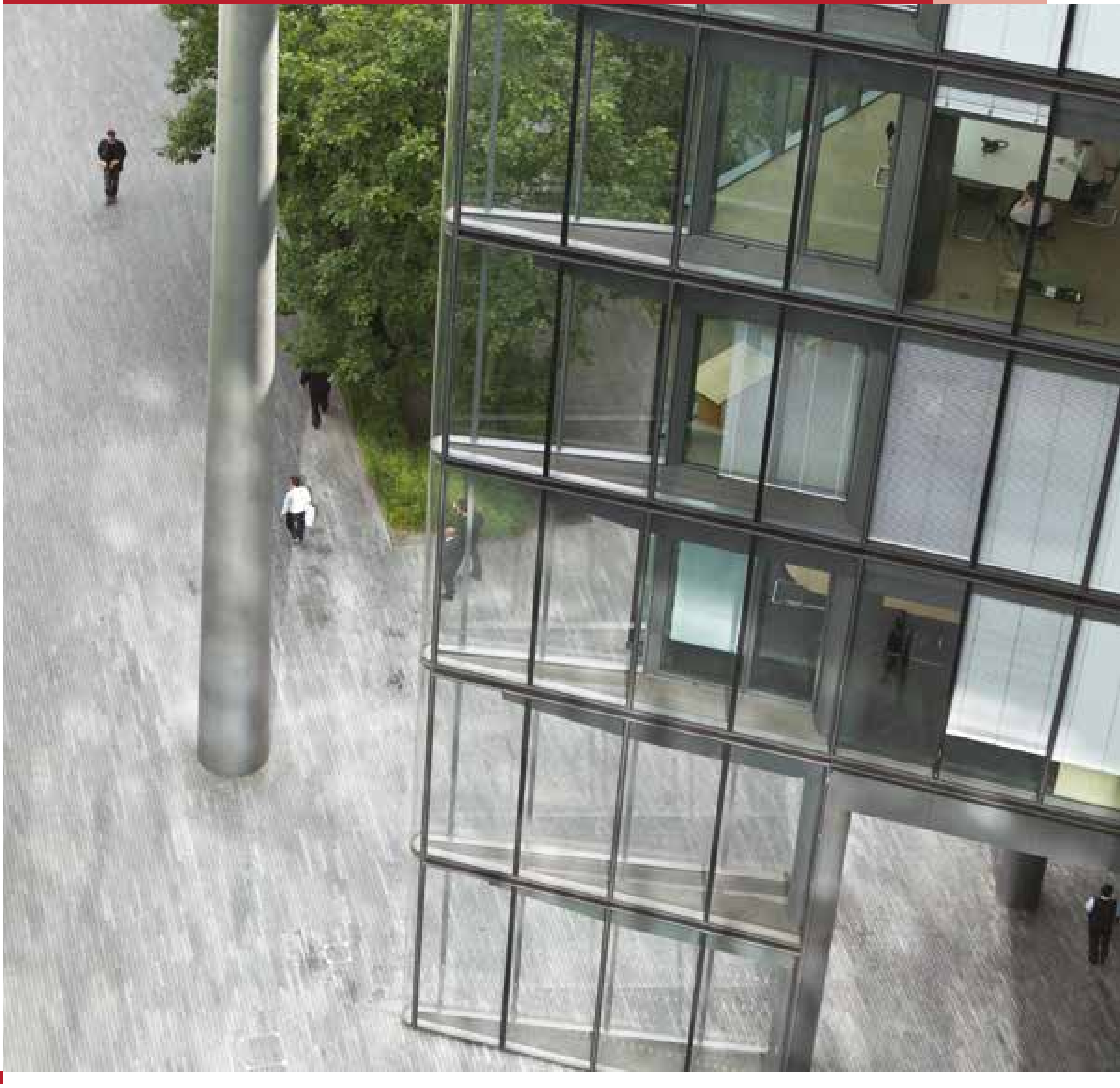
www.pwc.co.uk

Board discussions
What NEDs have been debating

March 2017



pwc

Contents

Introduction

PwC's programme for Non-Executive Directors (NEDs) 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 our September briefings on **General Data Protection Regulation (GDPR) and data privacy**. The GDPR is now in its final form and will come into force at the start of 2018, replacing the existing Data Protection Directive. It will transform the data privacy and protection landscape by putting all businesses at risk of fines and sanctions if they fail to protect personal data. Individuals no longer have to prove that they have suffered financial loss but can just cite distress.

An early evening event in September explored **Blockchain and its far-reaching implications for business**. This technology, which underpins the crypto-currency Bitcoin, presents far wider opportunities and challenges than simply disrupting business models in the financial services sector. It consists of 'blocks' of data in a digital ledger which, in turn, creates a single shared view of the blocks that every participant in the network can access simultaneously. Blockchain therefore has the potential to remove the need for a back office/reconciliation process and also eliminate the 'middleman'. As it is sector agnostic, the potential implications of this are significant.

Our October early evening briefing looked at **Tax – a reputational risk for every business**. There is heightened public, media and political interest in matters of tax policy and fairness. This brings significant reputational risk and has elevated tax to a Boardroom issue. The need to respond to a broad range of stakeholders means that Boards need to be comfortable that they understand and can appropriately articulate their company's tax strategy and how the associated risks are being managed.

Risk is a constant feature on the Board agenda, even more so in these uncertain times, and we continue to focus on different aspects of this topic. Our winter workshop season included sessions considering **Culture as a risk management tool and a licence to operate**.

Culture is currently an area of focus for regulators and others as society attempts to respond to a lack of trust in business. The workshops explored how the Board can influence and shape culture, bringing values to life, building trust with stakeholders and assessing, measuring and monitoring culture.

As one specific area of risk, the darker side of the relentless technology developments, such as Blockchain and data analytics, was focused on in our two **Cyber security** workshops. 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 allowed for a deeper dive into four key areas – developing a business perspective, assessing current state, improvement recipes and handling incidents and crises.

Investor activism and how to respond was explored in another of our workshops. Investor activism is increasing in the UK as volatile equity markets provide activist investors with opportunities to build stakes in undervalued companies. Boards can be hesitant to react but being on the back foot often makes it harder to respond effectively to shareholders further down the line. The session considered what characteristics an activist looks for in a potential target and how Boards might respond, both in terms of taking steps to prevent an approach but also what to do once one has happened.

Recognising that in today's complex and inter-connected business environment crises will happen, the workshop season concluded with a session looking at **Crisis management.** Getting crisis response right is not something that can be improvised when a crisis strikes and the capabilities that underpin that response take time to build. In today's social media driven world, Boards no longer have the luxury of time to consider their course of action and need to be able to put a previously developed, and preferably rehearsed, plan swiftly into operation.

Our January briefings revisited the technology angle looking at **Data analytics and its role in relation to strategy.** The world is at an inflection point where artificial intelligence and data analytics can help businesses make better and faster decisions. However, too often data analytics is used to analyse the past rather than predict the future and inform decisions. To become a data-driven organisation, leadership needs to set the tone and deliver on it, using predictive analytics to support strategic decision-making.

At a more macro level, in February we had **A global political update** from Eurasia Group. In these uncertain political times, this early evening event provided an overview of Eurasia Group's top 10 political risks for 2017 to further inform strategic decisions.

Developments for **Audit Committees** – which continue to have a full agenda – were not overlooked. A series of update workshops provided a regulatory update, a look at developments in corporate reporting and accounting, as well as a session considering user access management. The latter has become ever more important as the risk and threat landscape continues to evolve due to increasing interconnectedness.

For those on **Remuneration Committees** there were sessions exploring issues with executive pay, including public perceptions of inequality. Recent corporate governance developments and Government consultations aiming to address these were discussed. Consideration was given to what this means for Remuneration Committees in 2017 and beyond in terms of transparency, strategic alignment and flexibility, stakeholder engagement and fairness.

We also ran a number of interactive sessions throughout the year including a 'Game of Threats'™ cyber attack simulation, a 'False Assurance' film event with the ICAEW and various webcasts exploring topical business issues. We plan to include further interactive sessions in future programmes.

In all of the events there was considerable debate, with a sharing of ideas on the topics and discussion around the role NEDs can play. The combination of expert knowledge with the invaluable sharing of experiences with peers adds real value to these sessions, and I would like to thank all those NEDs who participated. 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

Andy Kemp
Chairman,
Non-Executive Director programme
andy.kemp@pwc.com
March 2017

A global political update

Political context is important for business as political stability encourages a positive outlook which has a knock-on effect on the economy. Political risk can impact all aspects of a company's business such as consumer sentiment, workforce quality and availability, taxes and foreign exchange. Proper planning and management of political risks can therefore help to drive commercial success, especially in emerging and frontier markets.

Presenter:

Sean West, Global Deputy CEO,
Eurasia Group
West@eurasiagroup.net

Global political update

The session was structured around Eurasia Group's top 10 political risks for 2017.

As initial context, it was noted that the world is becoming riskier. For the first time, Eurasia Group are using the term 'geopolitical recession', where a substantial series of events has dragged down the positive impacts of politics. For the last five years, Eurasia Group has been talking about a 'G Zero world', one without global leadership. This has now combined with a populist revolt against globalisation whereas domestic policies were previously permissive towards it. This negative trend in domestic politics in key economies combines with negative external conditions at the geopolitical level resulting in the geopolitical recession.

A geopolitical recession plays out over a much longer timeframe. In Eurasia Group's projections, few countries show encouraging signs over the next six months. In a sense, a neutral political environment is actually a positive outcome.

The world is therefore much riskier now politically than a year ago. The 10 risks, as assessed by Eurasia Group and explored below, are not meant to be exhaustive but are the highest impact events with a material likelihood of impacting business.

Independent America

This is not about the US becoming isolationist but unilateralist.

- Militarily, it's all about America and other nations will not necessarily be able to depend on US commitments.
- Economically, it's about industrial policy that squeezes countries and companies for better deals for US workers.
- Values wise, the US focuses on transactions rather than principles.

Currently, therefore, there is the absence of a unified West supporting democracy from the same point of view, as well as the potential for negative bilateral relations. Implications of an independent America include:

- chaos from an absent superpower – particularly in Europe and the Middle East
- weakening of global institutions – global fragmentation
- the rise of China and possible conflict.

China overreacts

Given its current leadership transition, China is not in a strong position to withstand trouble and will want to quell anything that makes its leaders look weak.

- With the 19th Party Congress and leadership transition, President Xi Jinping needs to appear strong.
- Hypersensitivity to external challenges (eg Hong Kong, Taiwan, North Korea, regional waters, Trump) may cause China to respond forcefully.
- The need to prioritise stability over difficult policy choices risks policy failures such as a re-inflation of asset bubbles.

A weaker Merkel

Merkel will be re-elected but with a smaller majority. Previously Europe's indispensable leader, she will be a weakened figure.

- Externally, Europe will be challenged by France's elections, Greece's finances, Brexit negotiations and relations with both Russia and Turkey.
- Domestically, Germany will be challenged by their refugee policy, terrorist attacks, corporate crises and populism with the Alternative for Germany gaining ground.

Merkel is increasingly becoming a lone voice for keeping Russian sanctions in place.

No reform

Some countries that were previously planning to reform will no longer.

- Modi (India) will not get land reform through and Nieto (Mexico) has achieved as much as possible.
- In Russia, France, Germany and China, reform must wait for political transition.
- In Turkey, Britain and South Africa, leaders are preoccupied with domestic challenges.
- In Brazil, Nigeria and Saudi Arabia, ambitious plans will fall short of what is needed.

China's anti-corruption drive still results in a positive political outlook for this country in terms of reform but other major economies are on a neutral or negative trajectory as far as reform is concerned.

70%

of Americans want the new president to prioritise domestic policy

Technology and the Middle East

Middle East legitimacy previously came from the outside and then from energy money with the US and allies ensuring security. However, this is no longer the case due to technology in the following respects:

- Energy – US technology such as fracking is destroying the Middle East business model, enabling new producers and competition.
- Connectivity – this enabled the Arab Spring but is now a threat. ISIS can use social media to inspire individuals anywhere in the world and access to the internet is encouraging the reinforcement of tribes.
- Cyber – Iran is less constrained and attacking Saudi Arabia. Regional terrorists will increasingly use cyber weapons to attack infrastructure.
- Automation – persistent unemployment due to technology eliminates the benefits of a demographic dividend.
- Forced transparency – brittle regimes need secrecy but everything is becoming more transparent.

Central banks get political

The independence of central banks has rarely been questioned but various leaders have been publicly attacking the rates policy.

- Western central bankers are therefore newly vulnerable to political pressures.
- The political support for the ECB to act if there are additional shocks will be more questionable.
- The US Fed will be affected, either through partisan appointments or public criticism, as Fed tightening policy and fiscal expansion run counter to each other.

The White House versus Silicon Valley

Many technologists have a different world view and will disagree with Trump plus refuse to respond to presidential requests. Differing views are seen particularly regarding:

- security versus privacy
- social media and fake news
- jobs versus automated production
- immigration and investment in science.

Despite the above, there are some positives. Tax reform, streamlined regulations and the H-1B visas are helpful to Silicon Valley.

Turkey

Europe is depending on Turkey regarding the refugee crisis and it also has a role to play in Middle East stability. However:

- Erdogan is using the state of emergency to tighten his hold on the judiciary, bureaucracy, media and business sector.
- In 2017, he will hold a referendum to win the executive presidency that he has been seeking.
- This will exacerbate economic problems, leading to a further PKK crackdown and worsening foreign relations.

North Korea

Usually there is little visibility over developments in North Korea. However, based on recent missile and nuclear tests, in 2017 North Korea is likely to have the capability to reach the West Coast of America with its weapons programme which is considered a red line. Previously, the US and China would work together to prevent this but Kim Jong Un has no interest in deal-making. Eurasia Group foresee two scenarios:

- Trump increases pressure and military threats against North Korea with secondary sanctions hurting Chinese banks and leading to a China-US crisis.
- If the US centre left government favours diplomacy with North Korea, South Korea may cancel its US missile order with possible Trump retaliation generating a crisis.

South Africa

There is currently a crisis within the ANC. Zuma's wife is likely to take over but reform will slow. Global institutions that care about South Africa are defunded and distracted. Trump will have no real interest in stabilising small African countries and Europe will not be in a position to. South Africa has previously aided regional security but will be less able to as a result of the economic impacts of ruling party infighting in the run up to the December 2017 internal conference. The region is therefore likely to become riskier.

Red herrings

Eurasia Group also covered off a number of issues that they consider to be red herrings that do not merit significant concern:

- US domestic – might be positive for the economy and markets in the short term.
- India versus Pakistan – both governments are focused on domestic issues and will look to avoid conflict.
- Brazil – lawmakers know that their only chance of staying in power in 2018 is to move towards modest economic recovery so pension reform may go through.

Implications for NEDs and the businesses on whose Boards they sit

Sean concluded by emphasising that political risk matters to NEDs as it affects every aspect of a company's business. Boards need a really good understanding of what is happening on the ground in territories where their companies are investing and should also assess the extent to which their five year plans depend on globalisation continuing. To gain an understanding of whether political risk is on executive management's agenda, NEDs can ask:

- Is the company well organised to detect and manage political risk?
- What are the processes and governance mechanisms in place to make sure politics do not disrupt company operations or investments?
- How do strategic planning efforts account for political risk?
- What is the company's track record on integrating political changes into forward planning?
- When entering a new market or making a strategic acquisition/ divestment, how well does management understand the political environment?
- How are expectations risk-adjusted on the basis of political changes?

Open forum Q&A

The open forum Q&A was wide-ranging.

One NED was keen to understand whether the Republican Party in Congress would put sufficient checks and balances in place against the effect of Trump who appears to be ruling by Twitter. Eurasia Group noted that the unpredictability is at least constrained by the legal system, as has been seen already with a judge ruling that the visa ban for Muslims from certain countries was unconstitutional. The Republicans are reluctant to stand up to Trump as it is rare to have one party control in the US government which is what they currently have and there are certain things they would like to achieve. However, they will back the judiciary.

57%

projected Grand Coalition in German government following election versus c80% currently

A question was asked around the reform point which showed the UK to be on a negative trajectory. This is because there is such focus on Brexit that it is difficult to think more broadly. There is talk of the two year process, following the triggering of Article 50, leading to a transition deal but this in itself may not be certain when all 28 other European territories have to agree to it.

One NED had a specific question on whether the far right party coming to power in the Netherlands would lead to a continuing 'Brexit' trend. Eurasia Group's view is that the Freedom Party will come first in the elections but will not form a government and so 'Nexit' is unlikely.

Another NED asked if Turkey represents a lost opportunity for the West. It is certainly a largely secular country with a sizeable population that could have been embraced. It is also a pivot state between Europe and the Middle East. Although Europe and Turkey are likely to agree on short term solutions to the refugee crisis, the possibility of long term collaboration is receding under Erdogan. Eurasia Group therefore agree that Turkey may well be one of 5-10 lost opportunities as globalisation is wound down.

There was interest in the Putin/Trump dynamic and how far relations with Russia would go. Eurasia Group's view is that Putin would actually have preferred a weakened Hillary Clinton as president due to Trump's unpredictability. Trump could easily change allegiance. Putin will play to Trump's ego in the short term to gain minor reliefs but there is unlikely to be the same harmony in 2-3 years' time. The Russian economy is reasonably sound and Putin has a firm control on the government. His main aim appears to be to disrupt the West and create an alternative view of where the world is going. Russia will not necessarily test NATO's resolve in the Baltic States but may do in other areas.

A NED enquired what impact dialogue between global leaders has these days when social media seems to be taking over. Eurasia Group's view is that this dialogue remains very important and contrasted President Bush, who held calls each week with key leaders, with President Obama who only talked regularly to Merkel. This had an impact on their respective influence on the global stage. However, at the same time, it is difficult to speak frankly if there is an increasing risk of leaks. There will be real cause for concern if diplomacy at an institutional level, such as the United Nations, breaks down.

c70%

internet penetration in Iran and Saudi Arabia.

There was a question as to why social inequality had not featured as a risk. Undoubtedly, there is currently a great deal of scrutiny on fairness, pay ratios, tax policies, etc and citizens will try and hold companies to account where they do not agree so Boards should be prepared for this. It was noted that some new business models almost create an 'addiction' (cf Uber and Air BnB) such that consumers will respond to attempts to curb their activities.

Another NED asked for some comments about oil, both in terms of pricing and the environmental issues. Eurasia Group noted that prices are recovering but more production will be brought online to control this, although they see a price of US$60/70/80 per barrel in the medium term. The climate change agenda has undoubtedly taken a step backwards with the election of Trump who will seek to backtrack from the Paris Agreement, possibly encouraging other countries to follow suit.

The final question was whether Eurasia Group thought Trump would be re-elected in four years' time. The view was that if he makes it to then he could be unstoppable but he may well not make it to this point.

Data analytics and its role in relation to strategy

The world is at an inflection point where artificial intelligence and data analytics can help businesses make better and faster decisions. However, too frequently, data analytics is used to analyse the past rather than predicting the future and informing decision-making.

To become a data-driven organisation, leadership needs to set the tone and deliver on it, with greater acceptance of experimentation. This was an opportunity for NEDs to explore some of the developments in this area and their implications for business.

Presenters:

Tom Lewis
tom.e.lewis@pwc.com

Oliver Bernath
oliver.bernath@pwc.com

Context

The session began with some context-setting. Intelligent use of data could help people and organisations to think laterally and use data to answer questions other than simply 'what happened?'. Today, there is a sea of information that tracks everything we do. Additionally, with the cloud, the cost of computing is collapsing so that extensive analysis is now feasible. Questions can be auctioned to providers who will bid to answer them. Organisations therefore have the opportunity to analyse anything but need to evaluate how much it is worth. A short film was shown to illustrate these points.

What data is there?

It is important to recognise that data is not just text and numbers. It can also come from emails, sensors in the Internet of Things and pictures. In fact, 90% of data is images and videos. Turning to some examples:

- Email histories can be used to analyse how people are interacting with one another (rather than what is in the emails). For example, this could illustrate whether a merger has been successful or whether there in fact remain two opposing sides.
- Sensors in the Internet of Things, such as 'nodding donkeys', can be used to predict when the equipment will fail.
- Pictures can be used to recognise whether documents have been signed.

Businesses should therefore consider where they can source data from and what they can use it for. One company used the shopping history of individuals from their smart phones to advertise relevant products or services on bins as they passed by. Additionally, the serial numbers of phones have been used to model how individuals use stations on their journey. Google uses phone GPSs to track when traffic is stationary and alert users of its route mapping products.

Companies should also consider whether they have a data asset others might want to buy. For example, some credit card providers pay a fee to phone providers to check the location of a phone if one of their cards is being used overseas as a means of verifying the legitimacy of this use.

A council in New York found that monitoring social media traffic on the state of public toilets was a more effective method of checking for maintenance issues than sending out a team of inspectors. This can also reinforce behavioural change if people notice that a problem is responded to promptly after a social media complaint.

The concept of a 'data lake' was briefly considered. Previously, if a report with certain data was required, the various parameters would be given to the IT department to create it. Now it is more a case of maintaining a data lake with any and all information in it, even if it is not currently known what the data may be used for, so that it is available should a need arise in the future.

As it is difficult to predict 'unknowns', the data lake can be trawled for relevant data once an 'unknown' has happened.

Clearly, there are privacy and other ethical issues relating to the storage of data, especially when an organisation does not yet know the use to which it will be put, and NEDs need to be mindful of these. It is, however, worth noting that the younger generation has a much more relaxed attitude to the privacy of data, preferring the benefits and convenience that sharing can bring.

Questions that NEDs might want to consider in the context of their businesses include:

- What data assets do we own?
- Are they accurate, complete, useful?
- What is the data used for? Is it valuable to others? Is it licensed?
- Does the company have a data lake? What is in it? Who uses it?
- Is it secure? Is it a risk? Who wants to steal it?
- Who is responsible for it?

The last question is particularly pertinent as the prevalence and value of data is too great for this to be left to the IT department.

30%

of UK companies are highly data-driven versus 53% in China

What do businesses use data for?

Data, often a combination of structured, semi-structured and unstructured data, can be analysed using algorithms and business models to generate a required output.

A model was discussed illustrating the data analytics delivery cycle where the following questions are explored:

- What value exists in your data?
- Can you trust your data?
- What happened and why?
- What might happen next?
- What is the right answer for your business?
- Is insight being delivered to the right people at the right time?
- How do you embed data analytics in your organisation?

As an organisation moves around this delivery cycle, it can progress from using data analytics to analyse the past to using it to predict the future and even to change the future in order to achieve a desired outcome.

It is, however, worth reflecting that advanced data analytics can be underpinned by some very complex maths. This often concerns users and so most big decisions are currently still being made with human judgement and the unconscious bias that this might involve.

Another short film illustrated some of the key findings of PwC's Global data and analytics survey 2016, involving more than 2,000 executives in 10 countries. These include:

- 23% of organisations are using data analytics to describe what has happened.
- 36% are using data analytics for diagnostics.
- Only 13% are using data analytics to automate decisions.
- Executives in data-driven organisations are 3x more likely to report significant improvements in their decisions.
- 30% of UK companies are highly data-driven versus 53% in China.

23%

use data analytics to describe what happened.

The UK is therefore lagging behind other parts of the world in terms of data-driven decisions. NEDs should consider their organisations' capabilities in this area. There are excellent products available to perform the analytics so this does not necessarily all need to be in-house. In order to think as expansively as technology makes possible, there is a need to combine instinct with analytics. It has been shown that productivity levels are much higher within organisations that are good at data analytics.

The session continued with a brief look at Artificial Intelligence and Machine Learning.

In the first machine age, the Industrial Revolution saw the automation of physical work. In today's second machine age, there is increasing augmentation and automation of manual and cognitive work. Part of this second machine age is the rise of Artificial Intelligence which is "intelligence" that is not the result of human cogitation.

Machine Learning is a subset of Artificial Intelligence involving the creation of computer algorithms that enable machines to learn through experience and acquire 'knowledge'. Typically Machine Learning is used to build 'models' that accurately make predictions or identify patterns from data.

Moreover, machines get better at learning really quickly as they are never off. Reference was made to an article in The New York Times Magazine entitled 'The great AI awakening'. This includes a description of how Google used Artificial Intelligence to transform Google Translate through the computer effectively learning by itself.

This was further illustrated by a picture of a heron. Trying to explain to a computer what a heron is in sufficiently distinct terms is very difficult but showing a computer thousands of images of a heron will enable it to learn for itself.

These principles can be applied in business. For example, having cameras on fridges in stores to see what products are being sold and to understand buying patterns, as well as the actions of the stockists. In the case of Brexit scenario modelling, computers can read contracts to model the impacts of various decisions.

It is important to recognise that computers have a point of view that is clean and non-biased. Today, computers are not just calculators but can see, listen and read. The Board of an organisation called Deep Knowledge Ventures already has some members that are algorithms.

36%

use data analytics for diagnostics

What does data analytics mean in the context of your business?

Questions NEDs might want to ask include:

- What decisions are we using data analytics to solve?
- How are we balancing analytics and experience in decision making?
- Who oversees the algorithms?
- Are we thinking out of the box enough?
- Do enough of our people think this way?
- How do we encourage innovation?
- How do we recruit, motivate, manage and retain these people?

Today's start-ups are already thinking very differently. There is a need to create the right balance between computers and humans, and the right culture for each to thrive, in order not to be overtaken by disruptors.

The session concluded with a brief look at three examples of real world uses of data analytics as follows:

- ***Hospital simulator*** – gaining deeper insight into a hospital's demand, capacity and process flow challenges and testing possible solutions.
- ***Trader intelligence*** – monitoring risks and reducing exposure to potential market abuse activities.
- ***Organisation design model*** – gaining a single view of an organisation's workforce.

Open forum Q&A

The open forum Q&A was wide-ranging.

One NED enquired about finding the right people able to do this and successfully bringing them into an organisation. It was noted that leadership is key in this area. Organisations have to be prepared to 'dream' and then attempt to convert the dream to reality which means being prepared to try and fail, as long as lessons are taken from the failures. Individuals with the deep mathematical skills required for advanced analytics can sometimes be introverts. They need to be given space once in the organisation and be recognised for what they are good at, rather than being moulded to 'the norm'.

Another attendee asked whether there is evidence of machines generating originality, flair and creativity. This is indeed starting to happen. For example, a US car manufacturer has fed in data from focus groups on why people like certain cars from an aesthetics point of view. Computers can work with this to design a car that a greater percentage of people will like the look of.

Equally, computers have begun writing music and it would be feasible for computers to be able to design the décor of rooms based on known preferences for colour, materials, etc. As with many areas, a diverse team is likely to be more creative.

There was a question around intellectual property and whether patent wars could become more frequent. However, an open source mindset dominates in this space. This leads to consideration of whether companies are needed in the same way today. Previously a corporate body was set up to raise capital, employ resources and provide premises but much of this can now be done online with auction sites used to solve problems. Effectively, people are being paid to do what they enjoy but, with everything so mobile, there can be a blurring between work and home.

There was a specific enquiry regarding questions a NED sitting on a healthcare Board might wish to ask. A good question for any Board is: "If Google was to enter my sector, what would it do?" or "Who is our fiercest competitor and what would they look to do?". NEDs can also ask:

- Are the business's leaders thinking about data analytics?
- Is it just lip-service or are thoughts being converted to actions?
- Does the business have skilled resources?
- If not, is it taking appropriate advice?

As mentioned above, Boards need to be prepared for failure but should ensure that the organisation learns from them.

Only 13%

use data analytics in a prescriptive manner to automate decisions

NEDs were concerned about the human dimension and whether technology is an invaluable aid or something that will lead to the 'de-professionalisation' of people's roles. At the same time, Boards may need to be considering whether it is negligent not to avail themselves of technological tools when others will.

In the future, there will undoubtedly be significant impacts on a large number of existing roles. It has already been shown that initial medical diagnosis can be performed very effectively by computers. Arguably, an individual in search of a diagnosis would prefer to benefit from data from every known scenario rather than a single doctor's brain.

There will, however, be difficulties to overcome along the way. For example, one of the biggest problems with driverless cars is that they are unable to comprehend that humans break the law and therefore do not all drive as predicted. Overall, however, the upsides in the area of data analytics are so vast that the downsides are likely to be ignored or rejected.

One NED enquired whether the governance of data analytics/data security/data privacy should all come under the CDO. It is right that there should be a role around the governance of information assets but this needs to be alongside 'data evangelists' who are prepared to test the boundaries. It is helpful for there to be a subset of the risk function that understands data analytics concepts and language. Over time, regulations are likely to adjust as people become increasingly comfortable in this space.

At a big picture level, there was a final question around which countries are doing this best if the UK is lagging behind. The west coast of America has hugely impressive resources attracted by, and prepared to work hard for, significant economic rewards. There is also real investment in this space happening in China.

General Data Protection Regulation and data privacy

The General Data Protection Regulation (GDPR) comes into force in May 2018, replacing the existing law, the Data Protection Directive. It will totally transform the data privacy and protection landscape as any entity of any size, public or private, anywhere in the world dealing with personal data of European (EU & EEA) origin will be impacted.

This was an opportunity for NEDs to have an overview of the far-reaching implications of this regulation.

Presenter:

Stewart Room
Partner, PwC, Global Cyber Security and Data Protection Legal Services Leader; UK Data Protection Leader
stewart.room@pwc.com

Context

The session began with some context-setting. Stewart first emphasised the sheer scale of this law as most other laws have 'perimeters' that ring fence and limit their scope. For example, employment law only applies to employers and employees. However, the GDPR gives rights to all living individuals whose personal data are in Europe and will affect the largest multinationals, most of the public sector and all the way through to small busineses, such as the window cleaner with customer details on their iPad. Some B2B deals are already featuring audit rights for data handling in contracts. It is highly likely that the regulation will give rise to more disputes/litigation once in effect.

It is worth noting that security is only one issue of the GDPR. There are many other key requirements ranging from transparency rules to rules on data quality and rules on how to build data protection compliance programmes. Many organisations are not ready for its impact. Although the GDPR comes into force in May 2018, it was first proposed in 2009 and promulgated in draft in 2012 so there will be little sympathy for those who are not ready by the implementation date.

GDPR and Brexit

The implementation of the GDPR will not be impacted by Brexit for the following reasons:

- It was the UK that initially proposed the law and the UK Government supported its passage through the EU processes.
- The GDPR comes into effect in May 2018 so will be in force before the end of the two year period that runs once article 50 is triggered.
- Trading with the EEA/EU will be conditional on the UK accepting the GDPR.
- UK based data importers and multinationals operating in the UK and the EU will need GDPR-type adequacy to avoid legal challenge.
- Multinationals operating in the UK and the EU will build to a GDPR common denominator.
- Domestic law is independently moving towards the GDPR's objectives (breach disclosure, distress compensation, marketing).

Moreover, the Government has announced in the Brexit White Paper that the UK will meet the standards of the GDPR after Brexit.

Background to the GDPR

Awareness around data protection has grown significantly since 2007. A relentless torrent of data and privacy breaches has affected the political, public and regulatory psyche. This can be viewed as a 'Regulatory Bear Market' with multiple bears (judicial, citizen, political, regulatory) uniting with significant impact.

As examples:

- ***News of the World*** – the 'phone hacking saga ultimately led to the demise of this organisation.
- ***Data Retention Directive*** – this regulated the holding of data by telecos and ISPs for security/terrorism purposes but was ultimately unwound having been deemed to breach human rights,
- ***Right to be Forgotten*** – an individual's request to have old data removed from a Google search affected Google's 'crown jewel' web search in Europe.
- ***Safe Harbour*** – this was dismantled following Facebook's transfer of personal data from Europe (Ireland) to the US (California).

All of the above examples illustrate how powerful the 'Bears' can be when they combine.

An advert from a firm of solicitors was used to expand on the wider background. A disgruntled internal auditor had left a major retailer taking an employee database with him. The individual was convicted and jailed but the solicitors initiated a class action for compensation against the retailer and almost 7,000 employees have signed up. This case is continuing through the courts.

The GDPR therefore came into being against this backdrop and the financial penalties can be significant with fines of up to 4% of an entity's annual turnover in addition to compensation payable to those affected in litigation.

Scope of, and points to note regarding, GDPR

The GDPR applies to any entity processing personal data of European origin. The definition of 'processing' is broad and includes adaption, transfer, sending etc, – really any act that can be performed to data except dreaming or thinking about it.

The key points to remember are:

- The GDPR is law to regulate the processing of personal data.
- All industry sectors are affected.
- The reach of the law goes beyond Europe – any entity worldwide will be caught if it deals with Europe.
- Lawmakers foresee significant problems with data protection and feel the market is not responding so are regulating accordingly.
- Financial risk is seen as the solution to the issue.
- Entities have to re-contract with their stakeholders.
- Repairs can be packaged up using a risk-based approach.
- Entities need to maintain trust in their digital futures.
- They will have to quickly remedy any problems given how long the GDPR has been in existence.
- However, entities can easily lose their way without appropriate support.

Given the amount there is to be done, entities will need to optimise their approach to address key risks. For most organisations, there is probably not enough time to map all data and come up with a full legislative compliance journey so it may be better to take a risk-based approach. As the law has legislated for a principle-based system, it is likely to be more effective to look at where harm might arise.

The GDPR is built around three key pillars

Transparency

This needs to be considered over the entire life cycle, right from prior to collection of the data.

- Entities need to be much clearer about how they use personal data.
- Consent rules have been toughened with new proof requirements (assumed to be none in the absence of proof).
- Access rights have been increased with a shortened delivery time (reduced from 40 days to 20).
- Mandatory breach disclosure requires entities to come clean after data breach cases and tell the regulator within 72 hours of detection of the incident and the people affected in serious cases without undue delay.
- Enhanced rights of regulatory inspections and audit will be introduced.

Compliance

The existing Data Protection Act in the UK has eight principles which will be expanded by the following new requirements.

- 'Privacy by design' means entities have to get data handling right from the start.
- 'Privacy impact assessments' will have to be routinely carried out.
- 'Accountability' means all data use and the related risks have to be documented.
- 'Data portability' permits people to take their data with them (e.g. when switching energy/insurance/financial services providers).
- 'Right to be forgotten' means that people will have greater power to demand deletion.

Punishment

- There are tougher enforcement powers for regulators.
- Financial penalties are up to 4% of the legal entitiy's annual turnover.
- Compensation rights exist for distress.
- Civil Society Organisations can sue on someone's behalf without the individual's consent.
- Data processors are liable in their own right.

The compensation point is particularly key as some of the most complex challenges in the regulation are likely to come from citizens. Individuals do not have to demonstrate financial loss or physical harm but can just claim distress. Given there are 500 million EU citizens and 28 EU Data Protection Authorities, this represents a huge potential financial exposure.

Considerations for NEDs

In light of the above, NEDs may want to consider two fundamental questions:

- How will their organisations deal and cope with the challenge?
- How will they be able to prove that their entities are 'good' (have appropriate systems and operations in place)?

500m

citizens in Europe benefitting from new rights and powers

Open forum Q&A

The open forum Q&A covered a range of issues.

One NED enquired how the UK compares to the US situation where class actions seem to be more frequent and there also appears to be more freedom re personal data. It was noted that in the US the law is harm-based (e.g. financial loss) whereas the UK is principle-based so the situation does not translate directly. The UK could mimic the US 'class action' phenomenon.

NEDs asked where the Achilles heel might be, particularly for small companies. This could be in the supply chain so there is a need for greater due diligence and stronger contractual relations as the data controller and the data processor will both have liability. There was also concern around the accountability and portability aspects.

Another NED enquired whether the Board could go to prison and it was noted that there are no jail sentences attached to the regulation, although there could be personal civil liability if a Board member connived or collaborated in the non-compliance or was guilty of neglect.

The NEDs were interested in how they can satisfy themselves that their entities are fulfilling their responsibilities with regard to data protection. Organisations need to take appropriate steps with regard to technical and organisational matters to ensure that they are on the 'bell curve' of the consensus of professional opinion regarding what is adequate.

28

EU Data Protection Authorities

The law will tolerate some failure if there are appropriate systems and processes in place. It will also be advisable to take a risk-based approach – for example, ensuring there is an appropriate script in place for dealing with complaints at a call centre may be more valuable than detailed mapping of data. Flashpoints are likely to involve compulsory breach disclosure and there is no 'de minimis' for disclosure (unless the data lost was encrypted) and marketing and 'surveillance' activities (eg monitoring actitivities online or other behavioural aspects).

A NED was interested in who should own this and it was agreed that this is not solely a legal or IT matter but needs to be owned by the business. The CEO also needs to be able to talk knowledgeably about data protection wherever it sits.

There was also interest in whether there is diversity across the EU in this area. It was noted that every member state has different laws currently and one aim of the regulation is to resolve this.

Another NED enquired about the interaction with other legislation, e.g. health & safety, an example being where an entity uses telematics to monitor phone use while driving. There is unlikely to be pushback where employee monitoring is for legitimate purposes.

NEDs enquired about the skill sets of the regulators and whether they are likely to be able to cope with the volume of reporting that may result from the GDPR. It was noted that skill sets have improved in recent years but resource constraints are likely to be an issue and so the regulators may have to make choices about where to focus.

There was some concern that unintended consequences of the regulation could lead to an industry growing up around compensation, as with PPI. This is a possibility as barristers and solicitors have been meeting to discuss the expected increase in cases post 2018.

One NED noted that the impact on people, customers and the business model when a privacy issue occurs is significant and NEDs need to be aware of this more broadly. It can often become a 'licence to operate' issue.

Finally a NED enquired if insurance could be taken out in respect of GDPR breaches. It is possible that insurance may cover some of the aftermath but it cannot cover regulatory fines. Additionally, individuals cannot contract out of statutory protection rights.

Blockchain and its far-reaching implications for business

Blockchain, the technology that underpins the crypto-currency Bitcoin, presents far wider opportunities and challenges than just disrupting business models within the financial services sector. It consists of 'blocks' of data in a digital ledger and is believed to be highly resistant to malicious tampering. The ledger also creates a single shared view of the blocks which every participant in the network can access simultaneously.

Blockchain therefore has the potential to remove the need for a back-office/reconciliation process as well as the requirement for a middleman, reducing cost, delay and risk. In addition, using digital identities to unlock the capacity of blockchain could lead to huge societal change by bringing the 30% of the world who do not have a legal identity into mainstream society. This was an opportunity for NEDs to have an overview of the far-reaching implications of this technology.

Presenters:

Patrick Spens, Director, PwC and Chair of the Governance Committee of the Whitechapel Think Tank, member of UCL financial computing faculty board, member of GovCoin systems advisory board, on global leadership team of ID2020, honorary adjunct professor of Macquarie University and an executive fellow at the Henley Business School
patrick.spens@pwc.com

David Moloney, Director, PwC
david.r.moloney@pwc.com

Context

The session began with some context-setting. Just as the internet had revolutionised the exchange of information, blockchain has the potential to revolutionise how we exchange value by creating trust on the internet. Currently, exchanging value on the internet requires a trusted central party because when value is represented digitally it can be duplicated or manipulated. For example, we instruct our bank to make a payment, the bank verifies we have sufficient funds and then makes the payment. Blockchain enables the distribution of trust which potentially removes the need for a trusted intermediary which in turn reduces cost, delay and risk.

How does blockchain work?

Blockchain creates a single trusted version of the truth using a distributed ledger, consensus protocols and cryptography. In simplistic terms, how it works is as follows:

- Someone in a network requests a transaction.
- The transaction is broadcast to other computers (nodes) in the network.
- The network of nodes validates the transaction using agreed consensus protocols.
- If valid, the transaction is combined with other transactions to create a new block of data for the ledger.
- The new block is added to the chain in a way that is permanent and unalterable.
- The transaction is complete.

This technology could be used in numerous ways beyond financial services such as supply chain provenance, land registries, airlines, etc. It requires a closed user group that sets the rules/protocols for the group.

Transformative potential of blockchain

A video was shown of a short extract of Patrick's appearance before the House of Lords Economic Affairs Select Committee to talk about blockchain. This illustrated the level of engagement the Lords had in the subject but also some of their concerns.

The distributable ledger technology that is blockchain is not new as the original code was released on the internet eight years ago and has been worked on by bright minds since. It is complex code and encryption but potentially transformative as recent headlines have demonstrated:

- Santander estimate banks could reduce costs by $15-20bn per year by 2022.
- A report by PwC estimates that insurers could save $5-10bn through faster and more accurate claims settlements and compliance checks.
- A report by the World Economic Forum highlighted the potential for blockchain to disintermediate the financial services industry and save 10% of global GDP ($7.5tn).

$15-20bn

savings per annum for banks

Dispelling some myths

Patrick continued by dispelling some myths that have developed around blockchain:

1. Blockchain is just for Financial Services – in fact, blockchain is industry agnostic. It requires a user group to set the rules and then enables the exchange of value with minimal settlement and credit risk. It can therefore be used in any organisation with a supply chain to eliminate the need for work orders, purchase orders, invoices, receipts, etc. Auditors, regulators and tax authorities could have read-only access to the information, all helping to reduce cost, delay and risk.
2. Blockchain is just about money – in fact, the technology can be applied to almost any business process across all sectors. For example, there will be European legislation within two years requiring all pharma companies to have a bar code linked to a central depository allowing an individual to identify a medicine as genuine.

Blockchain does four things:

- It removes the requirement for reconciliation/a back office.
- It removes the need for a middleman (e.g. insurance broker, travel agent).
- It provides immutable proof of provenance.
- It has embedded business logic.

Where could this go?

The Bank of England is excited about the distributed ledger technology and has its own blockchain lab. In addition, two ministers are in charge of delivering the eight recommendations in Sir Mark Walport's (UK Government Chief Scientific Adviser) report 'Distributed Ledger Technology – beyond blockchain'.

In respect of recommendation 2, considerable R&D across all sectors is already being carried out by institutions including the Whitechapel Think Tank (made up of regulators, Government, the Central Bank, banks, universities and Fin Tech organisations) and the Alan Turing Institute, exploring the art of the probable.

Brexit may have slowed things down but change is coming in the Government which has the largest back office in the country and the largest bank in terms of the DWP. The DWP is today engaged in South Manchester making its distributions via blockchain and turning fiscal utility into social utility. Although this may result in redundancies, there will be significant opportunities in R&D. Parallels can be drawn with earlier 'technology' developments, such as the spinning jenny, where higher productivity in fact led to the industry becoming more commercial and employing more people. In a similar vein, PwC employed more people after PCs were introduced.

Areas of concern

The House of Lords had three key concerns:

- monopoly
- security
- 'Big Brother'.

Monopoly will not necessarily be an issue as long as blockchains can interact (cf a Vodafone call to a BT 'phone).

Most issues with security have been due to the protocols established and the implementation rather than the technology itself. Bitcoin has survived despite many minds trying to crack it. Nevertheless, organisations will want assurance around the security of a blockchain implementation.

The 'big brother' issue is really a question of policy. As an example, concerns have been expressed about limiting benefit payments such that they can only be spent in food/housing stores. However, a similar policy has been applied in South America for many years.

10%

of global GDP could be saved in the FS industry

The art of the possible

The session finished with a look at what blockchain could mean for personal identity. The UN published their 17 Sustainable Development Goals with 169 targets in September 2015 and one of these is a legal identity for all. Currently 1.5bn people have no legal identity and 53m children born every year are not registered. Human trafficking is a big problem and ID2020 is a not for profit organisation set up to explore whether blockchain technology can be used to achieve the legal identity target.

Considerations for NEDs

Returning to business, NEDs may want to bear in mind:

- Blockchain is both industry agnostic and policy agnostic.
- If their company's 3-5 year plan has not considered blockchain, this should be revisited. It may be right that blockchain is not relevant but the question should at least be asked.
- Identity is the key that unlocks the technology of blockchain.

Open forum Q&A

The open forum Q&A was wide-ranging.

The NEDs were keen to understand why the encryption is so unbreakable. Any hacks/breaches to date have been due to flaws in the implementation set-up and not the technology itself. It often comes down to cyber security hygiene as there is no fundamental vulnerability in the blockchain technology. Implementation is the risky element and companies may want to seek assurance over this.

Another NED wanted to know who owns the data. This will be a policy decision and will also need to comply with the General Data Protection Regulation. However, it is likely that a state will be reached where digital identity needs to be owned by each individual who then grants access.

Given the technology has been described as immutable, NEDs were interested in how it would work if something needed to be changed. It is likely that different types of blockchain will develop over time. They may multiply initially and then stabilise to a few.

One NED asked if a distributed ledger is more resilient. It is because data is much less likely to be lost than if, for example, there are only two data centres. In a blockchain set-up, data could always be reinstated from one of the multiple nodes. It is also worth bearing in mind that Bitcoin is permission-less as opposed to blockchain which is permissionable. The technology is developing every day.

There was a concern that removing the middleman removes the 'neck of the hour glass' where there is an overview of what is going on. This could be counteracted by having accountants/ regulators as read only users where necessary. The question is probably one of whether current intermediaries add real value or just cost.

The supply chain application was queried in terms of a major organisation which might have sensitive intellectual property it wants to protect. If a prime supplier wants to protect IP, it may be possible to grant different permission levels to different suppliers. A supplier could also be excluded by changing the code which means they are no longer able to participate. The user group sets the rules.

The NEDs were interested in the likely timeframe to significant implementation of blockchain. This is unlikely to be far off, although an exact timescale is difficult to predict. However, once one company adopts blockchain, others will probably follow very quickly. The adoption is not hindered by technology but by behaviours. The take-up by the younger generation is likely to be much quicker as they are more familiar and comfortable with the sharing concepts. It may be tempting to begin with a 'middle ware' version, taking out some but not all business processes, but the risk is that a 100% adopter could then quickly disrupt the business model.

Finally a NED asked what this means for education. There may well be less administrative roles going forward and a greater need for technology skills. The Government is aware of this.

Sir Mark Walport, the Government's chief scientist, published a well-written report into the uses of the technology across government in January 2016.

1.5bn

people without a legal identity

Tax – a reputational risk for business?

Barely a day passes without news headlines publicly examining the tax affairs of business, with heightened public, media and political interest in matters of tax policy and fairness. This discussion has elevated tax to a Boardroom issue. NEDs need to be comfortable that they understand and can appropriately articulate their company's tax strategy and how the risks associated with tax are being managed.

This roundtable discussion led by a panel of experts was an opportunity for NEDs to discuss the direction of travel of the tax environment, the future of tax reporting and how they can influence the right discussions in the Boardroom.

Panelists:

Kevin Nicholson
PwC Head of Tax
kevin.nicholson@pwc.com

Giovanni Bracco
PwC Tax partner
giovanni.bracco@pwc.com

Stella Amiss
PwC Tax partner
stella.c.amiss@pwc.com

John Connors
FTSE 100 Group Tax Director

John Whiting
Tax Director of the Office of Tax Simplification and NED at HMRC.

Context

The session opened with some context-setting around the current interest in corporate tax affairs. It was noted that tax came more to the fore as an issue around five years ago as a result of a combination of factors:

- The fallout from the financial crisis.
- The politics of the time.
- The growth of social media, allowing stories to escalate more easily.
- The tax system being unable to cope with the modern business environment and new business models.

It is worth noting that the UK has been very much at the centre of this debate. Australia has now caught up to some extent but in European territories, such as France and Germany, interest has tended to be more subdued, while emerging economies are often more focused on tax fraud.

It is also worth bearing in mind that the debate in the UK has been very focused on corporation tax which is only around 7% of the treasury tax take (7-15% globally). For every £1 of corporation tax, the largest UK businesses now pay £4 in other taxes such as business rates.

A key reason why corporation tax has become a smaller part of the tax mix is that successive governments have reduced the headline rate and offered corporation tax incentives to maintain the UK's attractiveness for investment. In the current environment, businesses can find themselves harangued by the media for taking up the incentives offered to them. Arguably, greater transparency and understanding of UK tax policy could help relieve some of the tension and confusion.

While the media focus is on corporation tax, it is not the only tax that warrants Boards' attention. There is also significant risk in payroll taxes and indirect taxes such as VAT.

Previously, there was an inconsistent interest taken in tax by Boards as the tax department was often viewed as 'a bit of a mystery'. Now, however, NEDs view tax as another commercial risk and are getting more involved asking questions such as:

- Is there an appropriate strategy?
- Does the tax department have the right skills?
- Do we understand and agree on the tax strategy?

7%

of total tax take is corporation tax

The big test is whether Boards could cope with a 'Today programme' interview on their business's tax affairs. Tax is undoubtedly a reputational risk for organisations and many different stakeholders, including a company's employees, have an interest in it.

What we are seeing with our clients

Companies are recognising the benefits of increased disclosure on tax. There are also more transparency requirements, such as the need to publish a tax strategy. To some extent, putting together a tax strategy document is relatively easy, although some are too generic. A good tax strategy needs to be very specific to the business. Also, putting together the statement is one thing, the difficulty comes in operationalising it.

Tax authorities are following guidance coming out of the OECD in terms of a framework. Although the requirement for the tax strategy to be formally approved by the Board was removed, in practice Boards will still want to agree the tax strategy that is published on the internet. Boards are considering:

- Who takes responsibility for the strategy?
- What governance and systems are in place once the strategy has been set?
- How are they tested?

It is possible that country-by-country reporting may ultimately become public, rather than just being for the tax authority as currently. Disputes with tax authorities may then become more frequent.

Since 2010 as noted above, the focus has been on corporation tax but risk also comes with employment and indirect taxes.

Experience of a FTSE 100 tax director

The group tax director outlined how he felt the situation had developed over the past 6/7 years. Previously tax was viewed as a 'niche/specialist' subject to be dealt with by experts. The tax numbers in the accounts were flagged to the Board but the tax department remained a 'black box' responsible for compliance and some planning. Now it is very much a public issue and a Boardroom topic because of the public and government focus. Boards are having to take greater interest and proper processes need to be in place.

The fact that tax strategy now needs to be published means that the Board looks at tax more holistically. Whilst the group is entitled to be tax efficient, they will not engage in inappropriate structures and aim to work on a 'more likely than not' basis that an approach would meet both statutory and reputational requirements.

Country-by-county reporting also makes tax an issue for the Executive Committee and local reviews are performed, as well as a review at group level, looking at both on and off balance sheet matters.

There is more discussion of international tax developments and the potential impact on the FTSE 100 organisation, as well as discussions around brand and reputation. The whole conversation has therefore shifted from when it was just focused on the numbers in the accounts. The discussions at Board level are replicated at Executive Committee level and the whole process is more rigorous and satisfying.

An earlier suggestion that the international tax system is broken was queried. The arm's length principle remains appropriate but the difficulty is how to apply it in a digital environment.

Final points made were:

- NEDs have a key role to play and need to ask relevant questions.
- Transparency is key (the FTSE 100 group publishes more than required because they feel the context is necessary and it is also helpful to employees).

Views from a long term tax practitioner now working as a civil servant

Tax has always been a reputational issue but it has risen up the agenda because the government is short of money and there is a 24 hour media circus. Both of these combine to create political attention and pressure to do something about it.

A focus of the government has been on getting better at collecting taxes rather than raising tax rates and this goes for all taxes not just corporation tax. The 'tax gap', ie the difference between what should be collected and actual collection is £34bn which translates to 6% of total tax take. This is better than most other countries.

Avoidance amounts to around £3bn or 10% of the total but the biggest element is due to the cash/hidden economy and approximately 50% is due to small businesses.

The tax gap has remained reasonably constant in recent years in cash terms and so is a reducing % of tax take, as tax authorities have more power, focus and intelligence. However, pressure to close the gap further is still there. The government has been successful in conveying to business that paying the right amount of tax matters. HMRC operates a risk-based approach and it is therefore better for companies to take the matter seriously.

For CSR purposes, companies need to be seen to be good tax citizens and staff want to work for organisations with good ethics. Tax will therefore remain on the political agenda and needs to be on Board agendas.

34bn

= 'tax gap' between expected and collected tax

Open forum Q&A

The open forum Q&A covered a range of issues.

Given that campaigns often drive behaviour, one NED enquired where the next high profile campaign might focus. This could potentially arise out of country-by-country reporting, as previously the focus has been much more on UK tax. While it is not HMRC's role to be the world's policeman, it may be necessary to take more of a global view going forward.

Another NED noted that issues sometimes arose because of government to government matters, as with recent state aid cases. Corporates put their business operations in locations where there are incentives to do so but are then blamed for this or tainted by association. Going forward, it was agreed that there may need to be more international coordination. We are unlikely to get to a position where there is one overarching international fiscal authority but there may be more cooperation between different national authorities and more influence from the OECD, the World Bank or some other supranational authority.

Some participants thought future policy and debate may be influenced by potential changes to the US tax system, particularly in the area of double taxation. The occasional situation has been seen where a company has chosen to be taxed twice to avoid the reputational risk of being challenged. However, tax authorities may not all want to work together in a sensible way. The political aim will be to maintain competition and not give up sovereign rights to determine tax.

A NED noted that the Board has a fiscal duty to its shareholders and it was agreed that tax strategy as a whole needs to be debated at Board level. Companies need to be alert to the ethical debate, however, otherwise they will be challenged by their customers. It was felt that the AC Chair has a specific role in relation to compliance and control but values and reputation need to be debated by the Board. More companies now have tax as a reputational risk and there are good opportunities for NEDs to ask questions.

It was also noted that it is worth trying to broaden the debate to overall economic contribution and not just a narrow focus on tax. In Africa, the argument that the government has been deprived of significant tax revenues through pricing by multinationals has gained some traction but the overall picture in terms of employment and other economic benefits needs to be considered.

One NED raised the question of deferred tax which is often more complex due to the impact of possible future events. Full and transparent disclosure around deferred tax was agreed to be helpful.

Finally, a NED questioned whether there is evidence that HMRC is becoming keener to litigate. In fact, much of what is currently going through the courts is historical and HMRC are actually trying to avoid litigation. However, it is not yet clear what Theresa May's stance may be. Corporation tax discussions are unlikely to go away and deferred tax is poorly understood. However, it is equally possible that the next major issue could come from employee tax. The debate around tax, and the reputational risk involved, is therefore likely to continue.

Culture as a risk management tool and a licence to operate

Culture has been a focus for financial services organisations since the financial crisis but recognition of the importance of an organisation's culture is now becoming even more widespread across all sectors. Regulators are particularly interested in this area and, in July 2016, the FRC released a report on 'Corporate culture and the role of the Board'.

Culture can happen by default or it can be designed. A strong culture happens when it becomes a focal point throughout the business through setting clear purpose, vision and values which are aligned with the organisation's strategy. Ultimately, a company's culture will impact how it interacts with, and is perceived by, the external environment – culture is key to reputation.

PwC/third party experts:

Tracey Groves
tracey.groves@pwc.com

David Taylor
david.taylor@pwc.com

Mark Goyder
CEO, Tomorrow's Company

Richard Sermon
Chairman, City Values Forum

Oonagh Harpur
Board member, City Values Forum and Senior Advisor to Tomorrow's Company

This workshop began with a look at the context and some definitions to ensure that there was a common understanding of culture.

Context

There is no doubt that culture is important. This was illustrated by a number of statistics from a variety of surveys:

- 50% of the largest corporate bankruptcies were due to unethical business.
- 70% decided not to purchase a company's product because of its questionable ethics.
- 84% agree that their organisation's culture is critical to business success.
- 1 in 3 people have left a job due to disagreeing with ethical standards.
- Individuals are 38% more likely to be productive if they feel engaged in the role.
- 60% say culture is more important than an organisation's operating model.

Definitions were explored of concepts such as purpose, mission, values, behaviours, ethics and integrity – all of which are inputs leading to culture as an outcome.

In order to be able to address culture, there is a need to break it down to its constituent inputs which can then be used as levers to influence and inform culture. It was recognised that whilst values should be global in a multinational organisation, how they are manifested in different cultures may be affected by cultural norms and traditions. Indeed, the core understanding of values may vary in different cultures.

A model for organisational culture and behaviours was discussed where a company's purpose, vision, values and behaviours, reflected through decisions and ways of working, result in higher performance in terms of business results and outcomes. Looked at another way, business outcomes (including financial performance) come from good decisions with the right ways of working based on a company's purpose, vision and values.

In order to have some confidence that there will be the desired outcome, various behavioural reinforcers are required:

- leadership action
- communication
- people practices
- performance management and reward
- organisational structure
- external environment.

Financial targets and 'short termisim' can impede the 'right' behaviours and so leadership action and appropriate performance management and reward are particularly important. In order to drive a strong culture, alignment is needed between intention and these reinforcers. An informally developed culture without these aligned underpinning drivers may appear to work but may not be sustainable long term when pressures are brought to bear and business dilemmas emerge.

In order to identify when behaviours are misaligned, NEDs can consider questions such as:

- What does success look/feel like in terms of building a strong culture?
- How do we make decisions?
- How do we behave?
- What are the desired behaviours we are looking to achieve?
- What will that look/feel/sound like?
- How can we measure this? What would the key indicators be?

50%

of the largest corporate bankruptcies were due to unethical business.

A guide to Board leadership in purpose, values and culture

Representatives from Tomorrow's Company and the City Values Forum talked through their guide 'Governing culture: risk and opportunity?' and the related toolkit. It was noted up front that Tomorrow's Company's work on the Board mandate precedes this in terms of defining purpose, vision, values and behaviours. As stated above, there is now a great deal of focus on culture and getting culture right can add real value to an organisation.

Tomorrow's Company/City Values Forum's guide gives NEDs key questions to ask in this area – both of the Board and of executive management – set around six pillars:

- inspiring purpose and values
- aligning purpose, values, strategy and capability
- promoting and embodying purpose and values
- guiding decisions using purpose and values
- encouraging desired behaviours
- assuring progress is being achieved.

This is intended to be an iterative process as companies and the business environment will evolve over time.

For each of the six pillars, three levels are set out to help Boards identify where their organisations currently are and where they may want to get to. These range from being at the beginning of the journey through to being quite advanced in this area and this needs constant revisiting as the world and the organisation's own geographic footprint changes. Forcibly, the questions and the levels are somewhat generic and should therefore be tailored to an organisation's specific business.

The first two pillars above – inspiring and aligning – set the 'tone from the top'. In addition to the Board, it was noted that the CEO plays a vital role in this. There was some debate around whether the current joint stock model impedes this, through a focus on short term results. However, this was not seen to be the whole issue, although Boards could potentially help to shape discussions with investors more.

84%

agree that their organisation's culture is critical to business success.

Promoting and embodying considers how the tone flows down throughout the organisation and how people behave when out in the business. Embedding culture was illustrated by the example of a customer service awards event at a company where the CEO, over a period of more than 30 years, had never missed the ceremony.

Guiding decision making should be supported by clear processes. Having a triple bottom line – people/customers/results – can be more effective in terms of developing a good culture than pure financial metrics.

Encouraging desired behaviours is important and a culture of fear needs to be avoided. People need to be enabled to do the right thing and there should be repercussions/penalties for those that do not. However, this needs to be balanced with the need to encourage transparency when concerns arise.

The final pillar is around assurance. There are often a number of measures that can be looked at within an organisation (e.g. surveys, complaints, etc) and these need to be triangulated with the Board member's own experience and speaking to the head of HR, Compliance, Internal Audit, etc..

Boards should work out where their organisations are and prioritise where they want to get to. Culture can be a matter for specific focus at awaydays but should also be brought into all Board meetings. It needs to express the 'personality' of the business.

Lessons from financial services

Following the financial crisis, there has been a great deal of focus on culture within financial services. The FCA's 2016/17 business plan has a number of paragraphs addressing culture and states that "Boards have a critical role in setting the 'tone from the top'."

Regulated firms are being challenged to address four risks:

- Poor cultures in firms drive behaviours that result in poor consumers and markets.
- Firms' strategies, business models and governance arrangements are not aligned with firms' values and good conduct.
- Incentive structures and performance management do not reward behaviours that act in the long-term interests of customers and market integrity.
- Weak governance and lack of accountability create poor oversight of risks to customer and market integrity risks in how firms are run.

An Individual Accountability Regime is being instigated with three facets:

- The Senior Manager Regime.
- Certification Regime.
- Conduct Regime.

A key principle of individual accountability is that it will no longer be acceptable to say "I didn't know" in the event of an issue/breach.

The regulators are looking for greater interaction from NEDs and increased time commitment. Two of the prescribed responsibilities are:

- ***Responsibility H***: embedding the firm's culture and standards in relation to the carrying on of its business and the behaviours of its colleagues in the day-to-day management of the firm (typically assumed by the Chairman).
- ***Responsibility I***: leading the development of the firm's culture by the firm's governing body as a whole (typically assumed by the CEO).

The regime currently applies to banks and insurers but will apply to all financial services organisations by 2018. It has encouraged debate and clarity around what an individual is responsible for and given more focus to the escalation of issues. NEDs need to demonstrate they have taken reasonable steps in this area and part of this is consideration of the management information/data they have access to in order to get a feel for what is happening.

There was debate around whether a ‘regime’ encourages a ‘tick box’ exercise and a fear culture. It does, however, go some way towards guiding against systemic flaws, although one-off human mistakes may still happen. The spirit needs to be that individuals may still get things wrong but should not be actively doing things wrong.

A discussion around whistle-blowing suggested there may be concern if there is nothing being reported, although it was recognised that this is not the only route for raising issues and some individuals may go through their line manager where there are high levels of trust. Staff and customer surveys, exit interviews, complaints, etc can all be valuable sources of data, as can the informal networks that exist within an organisation.

1 in 3

people have left a job due to disagreeing with ethical standards

There also needs to be a balance between qualitative and quantitative assessment of the ‘speak up’ culture. Sometimes flagging everything can help to identify themes. A tolerant attitude towards errors is needed to encourage reporting but, at the same time, there needs to be a consequence for offences. Transparency is important.

What does this mean for NEDs?

The Volkswagen emission tests issue was used as a case study to further consider how NEDs might respond. Even before the matter became public, there were a couple of flags that something was not right – one from a whistle-blower and another from a university conducting some independent research. In 2012, the CEO made a public commitment regarding clean engines which the engineers knew was not achievable but they were too scared to speak up.

Boards sometimes find it difficult to challenge success, even when there is an element of knowing it may be too good to be true. The younger ‘millennial’ generation care about making a difference and Boards should find ways to tap into this. They also need to guard against group think.

Overarching questions NEDs can ask are:

- Is our culture in line with our strategy?
- What channels do we have for employees to report concerns and escalate issues?
- Are our new hires and existing employees trained and guided to be aware of the corporate values?
- Are we aware of our leadership biases/cultural blind spots?
- Do our policies, procedures and systems describe and drive the right behaviours?
- Are we incentivising good ethical behaviour and dealing with mis-aligned behaviour?
- How would we demonstrate to a regulator (or other stakeholders) that we are taking culture seriously?

Conclusion

In conclusion, it was noted that culture can happen by default or an organisation can design it. In order to do the latter Boards need to:

- Define their cultural aspirations in line with the company’s strategy.
- Assess their current state.
- Identify the behavioural priorities.
- Intervene to evolve and align culture.
- Monitor progress.

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
NED and senior adviser to PwC
sp@spmailbox.net

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.

However, there is a dark side to these exciting times with a dramatic growth in cyber threat over the last 2-3 years. Today there are more potential adversaries with more power, more access, more motivation and more impact. 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.

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:

- leakage of customer records (hundreds of millions)
- engagement of organised criminal groups shifting to a more aggressive posture (extortion, ransomware, etc)
- increasing scale and sophistication of attacks, especially in financial services (exploiting business processes)
- '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
- insider threat (corrupt, well-meaning, unintentional)
- continued rise of technologies which are outside the reach of law enforcement.

30%

of strategic risk registers did not include cyber risk

There appears to be 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 discussed. 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. 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.

The Board has a role to play in its direction setting role 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.

Results presented from client surveys demonstrated that, in practice:

- there is a mixed understanding of cyber risks and their impact at Board level
- risks are often delegated below the Board
- there is room for better communication between Boards and cyber risk owners
- skills, knowledge and understanding could be improved.

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.

Over 1/3rd

of companies believe they have had no security incidents in the last 12 months or do not know how many they have had

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 who could have a 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.

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.

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 willing to share intelligence with others?

29%

of companies do not think there is a senior executive who proactively communicates the importance of information security

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?

Each company will need to steer its own course taking well-reasoned risk choices and executing them well.

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

Kris McConkey
kris.mcconkey@pwc.com

Dr Stephen Page
NED and senior adviser to PwC
sp@spmailbox.net

This workshop began with NEDs discussing the impact of technology, and therefore cyber security, on every aspect of our lives from national defence and infrastructure to retail and health. It was agreed that Boards need to engage with this topic quickly and comprehensively.

There was a look at the National Crime Agency's cyber crime ecosystem which shows, 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, the Board's role in setting direction and assuring outcomes as well as the six confidences framework covering areas where Boards can seek to manage the risk – refer to the cyber security stage 1 workshop on pages 21 to 23.

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.

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.

90%

of CEOs are changing how they use technology to deliver on wider stakeholder expectations

Developing a business perspective

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.

68%

of CEOs back the power of data and analytics in understanding what the customer wants

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.

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 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
- % of supplier contracts with clauses for information protection
- % 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?

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.

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. There was some debate regarding how much the CEO can be relied on to assess this on behalf of the Board and when there may be a need to go direct to individuals. The individual responsible for the supply chain should have a view on cyber risk just as much as the individual who is monitoring fraud risk.

This sends a message that cyber is important to the Board.

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 crises

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 10 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.

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.

Questions the Board can usefully ask around handling incidents and crises are:

- How are investments prioritised between prevention, preparation, response and recovery?
- Has the Board recently practiced its response to a cyber crisis?
- 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)?

It was noted that regulations in Europe are changing such that the regulator will need 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.

223

days = typical time between cyber breach and impact

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 with 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 23.

Responding to investor activism

Investor activism is on the rise. Volatile equity markets are providing activist investors with opportunities to build stakes in undervalued public companies. We are used to seeing activist activity in the US but activist investor approaches are now becoming more common in the UK and their campaigns are increasingly public. Boards therefore need to be prepared.

Companies can be hesitant to react but being on the back foot often makes it harder for the company to respond effectively to shareholders further down the line. The workshop provided an opportunity to consider what characteristics an activist looks for in a potential target and how Boards can respond.

PwC experts:

Nick Rea
nick.rea@pwc.com

Abhi Shah
abhi.shah@pwc.com

Ralph Dodd
ralph.s.dodd@pwc.com

Context

The workshop began with a look at some of the major players in UK activism – Cevian Capital, Crystal Amber, Elliott, Harris Associates, Sherborne Investors and ValueAct Capital. It was noted that these often seek out campaign allies from major UK institutional shareholders. The activist investors are prepared to do considerable research which they then take to the institutional investors to support their case. Institutional investors are more frequently taking note and investing in activists or setting up funds. Some activists therefore already have funding or raise it while others are making the most of the liquidity in the market, leading to increasing capital at their disposal.

All this adds up to more UK companies having had some experience with investor activism, ranging from minor agitation through to a hostile bid. Activism in the UK has been a growing phenomenon, ever since the shareholder spring executive remuneration cases in 2012, with two activist events estimated to have occurred every week in 2016. This is likely to have been driven by low interest rates and uncertainty with investors looking for higher returns.

Activism is expected to continue based on an established trend in the US where it is much more prevalent, partly due to:

- weaker Board governance in the US
- less communication with shareholders
- proxies having more power
- greater visibility of shareholders on the register
- a degree of short termism.

Activists commonly seek Board seats in order to drive through their agenda. Actions have become more fundamentally about the Board/its strategy/changing its structure than tinkering with financial or operational areas. Often activists come in and take an executive position or have a name in mind and it is not uncommon for the existing CEO or Chairman to depart.

Activists have been targeting companies in every sector, including major household names such as Rolls-Royce, Electra, BP, Royal Mail, Reckitt Benckiser, AstraZeneca and Alliance Trust but will go after companies of all sizes where they perceive there is value to be had. Activism is therefore sector and size agnostic.

2

activist events per week in UK in 2016

80% of activist approaches in the UK in 2015 were in the mid, small cap and micro sectors, possibly because the potential opportunities are larger, the companies themselves have fewer resources and the activists can acquire a larger stake with their funds. Often there is an uplift in the share price on initial involvement. However, whether the benefit is sustained over the long term once the activist has left is more mixed.

There was some discussion around whether Boards had become too focused on compliance and not enough on strategy and performance. However, whilst this might be one reason for the rise in activism, it is also possible that Boards aren't communicating their strategy well enough to shareholders, including the timeframe for achievement, in order for the company to be given the chance to deliver on the strategy.

Each campaign is different but typically activists use a series of common tactics that companies often significantly underestimate:

- research potential targets
- acquire stake and build
- engage Board and demand change
- full campaign (public or private)
- AGM/meeting, Board seat and strategic review.

As a result of their extensive research, activists often have more detailed analysis than is available in internal papers. Strategy is often not fully developed at a company – Boards and executives may be preoccupied with operational aspects and approach it with an operational lens rather than from a value perspective.

Activists are often prepared to make public statements about what they aim to achieve as they are not held to account in the same way as corporate directors, at least prior to having a seat on the Board. They will try to engage the Board first but may go public if they feel progress is not being made.

Case studies

An activist approach can be very distracting for management. PwC has developed a unique shareholder risk value diagnostic that evaluates a company's performance against its global peers across a number of markets using operational, structural and governance metrics. The tool highlights the extent of a company's vulnerability to investor activism and the results help to articulate the company's performance as understood by the market in order to inform its investor communication strategy.

This was illustrated by a couple of case studies using information in the public domain. In both cases, the activists took a fairly long-term view and eventually managed to secure their desired Board seats to effect change.

>1,000

activist events expected in the US in 2016

Characteristics of potential targets

The workshop then considered 10 characteristics of potential targets as follows:

- shareholder value record can be challenged (existence of a 'management discount'?)
- concentrated ownership (top three shareholders own c20%?)
- announced merger or acquisition ('strategic acquisition'?)
- management's track record can be criticised ('corporate myths' recently exposed?)
- inefficient balance sheet (current WACC/gearing unjustified?)
- complex group apparently lacking strategic focus (intra-group synergies not exploited?)
- scope for portfolio optimisation/ rationalisation (value erosion in non-core assets?)
- intrinsic value not fully recognised by the market (unconvincing standalone strategy?)
- operational under-performance (underperforming peers?)
- corporate governance can be criticised (executive remuneration?).

If a CEO or Chairman is saying that a company is undervalued, it is important that the Board understands and can communicate why there is a difference.

Tips for preparing and responding to activist investors

A Board should prepare for an activist approach as they will be under pressure once it happens. The activists will have a game plan and the first meeting is very important. They may give the impression that it is just a casual chat but it is best to over-prepare. The Board should also be prepared to read between the lines, as the activists may hint at their plans, and should demonstrate that they are taking any concerns seriously. Activists often publish their research on the internet and this can provide helpful insights. Boards can be better prepared by:

- having a clear view on their valuation (and communicating it better to shareholders)
- being prepared to defend against the company's vulnerabilities by understanding where they are and what the strategy is to change them
- having a team in place to react quickly to an activist investor/hostile bid.

Final questions a Board can consider in this space include:

- How would an activist investor view our group as an opportunity?
- What plans do we have to address potential opportunities and vulnerabilities that could be exploited by activist investors?
- How would we respond if an activist contacted us?

2/3

campaigns are undertaken in private

Crisis management

Getting crisis response right is not something that can be improvised at the time a crisis strikes as the capabilities that underpin any response take time to build. In today's social media driven world, Boards are being pushed to respond rapidly and strategically to major crises, even while the organisation is still forming its operational response. They therefore need to be able to put a previously considered, and preferably rehearsed, plan swiftly into operation. Getting crisis response wrong goes beyond significant financial pain and affects reputation and relationships.

The workshop provided the opportunity to discuss a number of issues relating to crisis management including the link to the Board's risk appetite, building the right crisis capability, communication with internal and external stakeholders and testing response plans.

PwC experts:

Paul Robertson
paul.x.robertson@pwc.com

Claudia Van Den Heuvel
claudia.d.vandenheuvel@pwc.com

The workshop began with a look at why crisis management is important. There is considerable evidence from a variety of sources that illustrates that the scale and frequency of crises are growing and will continue to have a big impact. Examples include, but are not limited to:

- cyber breaches
- natural disaster losses
- product recall fines
- regulatory breaches
- terrorism.

Definition of what constitutes a crisis is difficult because it will depend on individual circumstances. However, a good starting point would be something non-routine that requires significant involvement of the senior management team. A crisis is not just a big incident that may be part of doing business, although it was noted that a major incident can become a crisis because of the impact of social media. The ongoing implications can be substantial in terms of relationships and recruitment, particularly among millennials who may be more attuned to 'social capital'. Equally, an organisation that has accrued social capital tends to be given more leeway when a crisis strikes.

It should also be borne in mind that crises can give rise to opportunity. An example was the recall of Tylenol after it had been tampered with on the shelves of retailers. Rather than dismissing the issue as a retail problem, the company took back all the product and then introduced new tamper proof packaging. This ultimately led to them gaining market share. Another opportunity that sometimes comes from a crisis is the ability to implement organisational and cultural changes more easily.

Types of crises

A graph was used to illustrate different types of crises.

- ***Classic rapid onset event, e.g. fire, flood*** – most plans tend to be designed around this and are very operationally focused.
- ***Hidden crises*** – these tend to already be very serious by the time they come to light which makes the time to respond even shorter.
- ***Operational disruption*** – this can often bubble along at a low level before something happens to make the issue develop into a crisis.
- ***Strategic disruption*** – this can arise where the business model is flawed and should be challenged.

When thinking about these various potential crises, Boards need to assess them against their risk appetite. It can be possible to develop metrics to indicate when vulnerabilities are developing – for example, having more than 14 expatriates working in a danger zone if the private jet only takes 14.

It was noted that, when dealing with crises as opposed to ongoing risk management, likelihood is of less interest. A remote event has the potential to be a crisis if it could bring down a company. Ensuring that the reporting of bad news is enabled within an organisation is important so that matters are identified at an early stage and escalated appropriately.

A further graph illustrated that the premium for companies that recover well from a crisis over those that do not is around 22%.

66%

of CEOs believe their business faces more threats today than 3 years ago

Views from CEOs

A pulse survey on crisis management recently undertaken with 164 global CEOs from firms of a range of sizes found that:

- 65% of CEOs had experienced at least one crisis in the last three years.
- In 91% of those cases, the CEOs felt it was up to them to lead the response.
- 64% of those CEOs had experienced more than two crises and 20% had experienced more than four.
- 40% of those CEOs expect at least one crisis in the next three years.

Despite feeling they were expected to lead the crisis response:

- 57% of the CEOs consider their business to be vulnerable because of out of date plans.
- 65% feel vulnerable about their ability to gather accurate information quickly in a crisis.
- 55% feel vulnerable about communicating with external stakeholders in a crisis.
- 47% feel that an unclear definition of what constitutes a crisis will lead to a poorly handled response.
- 38% feel vulnerable over a lack of clarity as to the responsibilities of the management team.

While being in charge and concerned about their plans and ability to respond:

- 21% plan on starting a programme to address this in the next 12 months.
- 25% have not started a programme or have decided to accept the risks instead.
- 30% have plans in which the CEOs have confidence.

>US$ 375bn

economic losses from cyber crime in 2014

The lack of planning is concerning, particularly when social media limits the time there is to come up with a considered response. Preparation is therefore vital. An engagement response based on stakeholder mapping is required and this needs strength in depth across a range of domains, e.g. legal, operational, communications.

Crisis management should not be driven by the public relations team, even though communication is an important element. Stakeholders will want to hear from the senior management of the company and so having media training in advance can be a useful element of preparation.

A crisis response will not be linear but will 'ebb and flow' in different areas at different times. Equally, a Business Continuity Plan is not the same as a crisis management plan even though many companies often think it is since these generally focus on operational disruption, often due to an insurable risk.

NEDs should be part of the crisis management plan as an additional capability for the executive team to draw on. They can also take the role of the 'strategic thinker', looking ahead to other possible repercussions whilst the executive team are having to focus on the immediate issues. Simply asking the executive team how they can help may make the NEDs more accessible.

As business today generally operates through an extended enterprise with outsourced business models and a variety of partners, it is vital that relationships have been developed with any third parties in the supply chain/customer base before a crisis strikes. This will ensure that there is an appropriate contact who will help with the response.

Crisis management standards

The contents of the recently-developed British and European standards (BS 11200 and CEN TS 17091) were discussed. These both suggest that crisis management is at least 50% preparatory. The proposed Crisis Management Framework splits the activities between preparation – anticipate, assess and prepare – and response which includes respond and recover. Supporting both of these areas is a 'learn and review' process from:

- actual crises experienced
- others' crises
- near misses.

The British standard is more advisory and a measure of professionalism in this area whilst the European standard is moving towards developing a more 'testable' process with indicative elements that would be expected to be in place. Neither have been tested in a court of law but NEDs should be aware of the standards as their company's response to a crisis may be viewed with these in mind.

The attributes of a crisis-prepared organisation

There are some key attributes of a crisis-prepared organisation:

- Existing and emerging risks are proactively identified, mitigated and monitored.
- Crisis tools and technologies are in place and understood.
- Leadership promotes an organisational culture that empowers action and quick decision making during a crisis.
- Leadership encourages continuous improvement of its crisis capabilities.
- Leaders and crisis responders are 'battle-tested', trained and exercised.
- In-house crisis capabilities, vulnerabilities and gaps are understood and addressed.
- Roles and responsibilities exist and are understood.
- There are clearly defined response priorities.

Increasing maturity in crisis exercising programmes is important. For example, a more mature crisis scenario exercise might be run alongside the day job as this is what would happen in reality. There also needs to be some 'exposure' training, e.g. knowing what systems do in advance in case there is a need to turn something off in the event of a cyber breach.

Clear responsibility should be set regarding when there is a need to escalate matters. There are often some clear 'black or white' cases but there is a need to manage the 'grey', where judgement calls will be required. It should be possible to establish a delegated authority framework, as often exists for financial aspects.

There was a discussion around the psychological impacts of a crisis. Under stress, an individual's ability to think wider narrows and people also tend to become more risk averse. They may request more information before making decisions and delay taking action. Individuals therefore need to be empowered to make decisions in line with the organisation's values based on information available at the time.

Individuals should also be aware of the tendency to be biased towards more recent information which can make teams react to the latest thing that has happened rather than following a predetermined plan. There will also be a tendency for people to deal with the areas they personally feel comfortable with when there is sometimes a need to rise above this and see the bigger picture. A key question to keep in mind is "Have we made decisions that are true to our values?".

Indicators for NEDs of a mature crisis capability

A selection of indicators NEDs can look for to assess the maturity of an organisation's crisis capability was discussed in four key areas:

Incident response framework

- Are values and principles clearly defined and communicated which guide the business-wide response to an incident?
- Have response teams, levels and members been clearly defined?
- Do people understand the touchpoints between all response teams?

Tactical and strategic policies, plans and procedures

- Are there updated plans in place to support the tactical and strategic level response to an incident or crisis?
- Do the plans set out an operating rhythm that defines how the right people will be brought together to respond across the business?
- Do the plans define how teams should assess the impacts and implications, make decisions, coordinate and manage all stakeholders during a response?

Competencies

- Are existing and emerging risks proactively identified, mitigated and monitored?
- Are responders well versed in managing uncertain information to create situational awareness and understand short and long term business impacts of a crisis?
- Does leadership empower action and promote quick decision making during a crisis?
- Do teams and team members work well together to coordinate a business-wide response and communicate in a controlled manner internally and externally?

Crisis exercising programme

- Has a programme been implemented to assess and continually improve the effectiveness of plans and procedures for incident response and crisis management?
- Are training exercises designed to build the capabilities and confidence within the teams required to respond to real incidents?
- Are exercises designed to simulate a realistic response and enable responders to 'learn by doing' by actively making consequence-based decisions?

Final overarching questions for NEDs to ask include:

- How would the business identify a potential crisis and who would take charge?
- Is that documented, validated and assured?
- How are investments between prevention, preparation, response and recovery prioritised?
- Does a preparatory function exist and what is their role?
- What would happen if the organisation suffered a major crisis tomorrow? How would they respond?
- What are the expectations of the Board and their role?

US$ 194bn

insured and uninsured losses from natural catastrophes (10 year average to 2014)

Executive remuneration

Executive remuneration remains an area in the media spotlight. A number of perceived issues have been identified by the public, media, politicians and shareholders and there have been several recent corporate governance publications and Government consultations seeking to address these. At the same time, there is the increasing influence of proxy investors to consider.

All of this is happening at a time when many Remuneration Committees will be seeking approval for an updated remuneration policy as these were set for three years in 2014 under the new remuneration regulations at the time. The workshop provided an opportunity to reflect on the many developments in the area of executive remuneration and the potential implications for Remuneration Committees in 2017 and beyond.

PwC experts:

Marcus Peaker
marcus.peaker@pwc.com

Fiona Camenzuli
fiona.camenzuli@pwc.com

Einar Lindh
einar.lindh@pwc.com

The workshop began with a look at current public perception of executive pay. Findings from a 2015 British Social Attitudes Survey across all income groups included:

- 59% believe there is one law for the rich and another for the poor.
- 60% think ordinary people do not get their fair share of the nation's wealth.
- 53% feel big business benefits owners at the expense of employees.

A number of issues have been identified by the public, media, politicians and shareholders specifically in relation to executive pay:

- Executive pay encourages short-term behaviour to the detriment of the British economy.
- Executive pay is disconnected from the pay of ordinary people and is threatening social cohesion.
- Current rules do not give shareholders adequate control over executive pay practices.
- Shareholders are not adequately engaged in the stewardship of companies.

There is real political impetus to respond to the public perception of lack of fairness, although PwC's view is that more regulation and policy is not necessarily going to help. Following the financial crisis, there has been a great deal of attention on this area with many focusing on the gap between CEO pay and that of the average worker. This has widened partly because of the increasing scale and complexity of business and there may not be a full understanding of today's CEO role. In a recent PwC survey, the public had a reasonably accurate idea of what CEOs are paid but felt they should get considerably less than this. European countries are less fixated on this issue, although there is increasing interest from the public and government, but it has been a cause for concern in the US for some time.

59%

of the public think there is one law for the rich and another for the poor

Governance developments in executive remuneration

There have been a number of corporate governance developments since summer 2016 including:

- The Executive Remuneration Working Group on pay simplification (July 2016).
- Updated GC100 Guidance on Remuneration Reporting (August 2016).
- High Pay Centre/Chris Philip – Restoring responsible ownership (September 2016).
- Updated LGIM Principles of Executive Remuneration (September 2016).
- BIS Select Committee Enquiry (response deadline October 2016).
- Investment Association Principles of Remuneration (October 2016).
- Hermes Remuneration Principles – Clarifying Expectations (November 2016).

The BIS Select Committee had questions on executive pay, directors' duties and the composition of boardrooms. Five specific questions were asked in relation to executive pay:

- What factors have influenced the steep rise in executive pay over the past 30 years relative to salaries of more junior employees?

- How should executive pay take account of companies' long-term performance?
- Should executive pay reflect the value added by executives to companies relative to more junior employees? If so, how?
- What evidence is there that executive pay is too high? How, if at all, should Government seek to influence or control executive pay?
- Do recent high-profile shareholder actions demonstrate that the current framework for controlling executive pay is bedding in effectively? Should shareholders have a greater role?

PwC's view on the current framework is that an advisory vote is better than a binding one. However, one proposal could be that if a company gets a vote of less than 75% two years in a row, then it has to have a binding vote on executive pay.

More recently BEIS published a Green Paper on 29 November 2016 with a White Paper due before summer 2017 and any regulatory change expected to take effect during 2018. As noted above, PwC's view is that more regulation is not necessarily going to help and indeed previous regulation may have been part of the problem with increased disclosures having a ratcheting effect by encouraging companies to pay the median.

However, change is definitely coming as political will supports this. The BEIS consultation focuses on three key areas – executive pay, worker representation and private companies (the latter more from an overall governance perspective). The six key questions on executive pay were discussed along with PwC's initial views:

Do shareholders need stronger powers to improve their ability to hold companies to account on executive pay and performance?

The current system of binding and advisory votes already gives shareholders the powers they need in most cases. Any reform should be focussed on the small number of cases where companies either lose a vote or achieve consistently low levels of shareholder support. A targeted approach based on the escalation model which would affect only those companies that had consistently received a low level of shareholder support would be the most practical approach.

Additionally, most investors have indicated that they would not use a binding vote on executive pay.

Does more need to be done to encourage institutional and retail investors to make full use of their existing and any new voting powers on pay?

There could be benefits in mandating the disclosure of fund managers' voting records. It is difficult to see how any shareholder committee model could operate successfully given the nature of the UK capital market where a number of large shareholders predominate, the increasing number of overseas investors in UK companies and the unitary Board structure in the UK which the Government has been clear is a successful model it has no desire to change.

The BEIS Green Paper does not address the role of proxy agencies which is an important issue as a vote against by ISS in the recent AGM season cost 35-40% of the vote since much of the tail of the register will follow their recommendation. Given their power, it may be appropriate for ISS to start indicating which way they will vote so that companies know what they are dealing with.

53%

feel big business benefits owners at the expense of employees

Do steps need to be taken to improve the effectiveness of Remuneration Committees and their advisers, in particular to encourage them to engage more effectively with shareholder and employee views before developing pay policies?

The existing model of shareholder engagement works well but the extent to which employee views are heard remains a weakness. The use of some form of Fair Pay Charter would be a practical way for companies to do more in this area.

A Remuneration Committee chair should have an appropriate level of experience but we do not consider it a necessary requirement for a chair to have previously served on the Remuneration Committee of a specific company before chairing the Committee of that company, as has been suggested.

Should a new pay ratio reporting requirement be introduced?

While publishing pay ratios might be the right decision for some companies, there is a danger that it could lead to misleading and unhelpful comparisons across companies. For example, comparing pay ratios between a hospitality company and a bank will offer little actionable data and is unlikely to lead to any real change. A more meaningful approach would be the publication of some form of Fair Pay Charter or narrative where companies explain the principles of pay in the organisation and how these link to decisions on executive pay.

Should the existing, qualified requirements to disclose the performance targets that trigger annual bonus payments be strengthened?

In our view, investor pressure has been effective in changing behaviour in respect of performance target disclosure and the majority of companies now provide a good level of information.

How can long-term incentive plans be better aligned with the long-term interests of quoted companies and shareholders?

It is crucial that incentives are designed to support long term behaviour and sustained business performance. The best way to ensure this is to design plans (which would ideally be simpler) so that executives become significant shareholders for the long term. However, clearly there is more than one way to achieve this, and any policy developments should encourage the adoption and use of principles rather than prescribe any particular models.

There is a suggestion that performance vesting periods might move from three to five years but setting targets for three years is already challenging and such a move may make executives focus more on salary plus bonus and discount long-term incentives more than they do already. A lock-in post vesting may be more workable, although average CEO tenures are not lengthy.

What is clear in all of the above is that the Government does not want to be mandating quantum.

Key themes arising

From all the recent reports and developments in executive pay, there are four key themes emerging:

Transparency

Here the aim is to improve the quality of remuneration reporting and use it as an opportunity to build trust amongst shareholders, employees and other stakeholders. In the various guidelines and recommendations issued, this is being addressed via:

- Greater expectation of retrospective target disclosure.
- Maximum salary must be stated in monetary terms or otherwise.
- Benchmarking peer groups should be consistent and fully disclosed.
- Shareholders expect Remuneration Committees to take a balanced view on the use of discretion.

The aim is more communication of context and not just compliance. The remuneration report should provide insight into how pay outcomes have been reached and how these relate to the rest of the workforce. Looking to the future, the report may become a two part document with communications in the front end and a compliance appendix. The aim should be to explain the context for pay decisions in the Remuneration Committee Chairman's statement. It may also be appropriate to more fully reflect the link to strategy here as there is no guarantee that a stakeholder will read the whole of the annual report and accounts.

Strategic alignment and flexibility

This area links to the complexity of CEO pay and pay for performance. If pay is genuinely aligned to strategy, the current 'one size fits all' approach is unlikely to be appropriate. Currently only 10% of the FTSE 350 have non-standard arrangements, with the standard being base pay plus an LTIP with a three year vesting period and often a two year holding period post vesting. Shareholders should trust Remuneration Committees to go outside of normal pay structures. Suggestions in the reports on how to address strategic alignment and flexibility include:

- More flexibility to choose a remuneration structure appropriate for the company's strategy.
- Endorsing the use of restricted stock with the right safeguards.
- Executives should have meaningful equity holdings while employed and thereafter.
- Simpler package designs whilst ensuring pay delivered reflects the change in long term value of the company.
- Increased shareholding requirements/clearer expectations of shareholding requirements.

Looking ahead, high and long-term shareholding with phased release coupled with lower emphasis on performance vesting, ie increased use of restricted stock, probably with an underpin, could become the new model. The example of two FTSE 100 companies that had both introduced restricted stock plans, one where the resolution failed and the other where it was passed – in part because there was an underpin – was discussed.

The right structure is more important than quantum and long-term shareholdings do have a positive impact on behaviour. However, a different 'same answer' may not be better than the existing 'same answer' as a company's pay structure needs to reflect its strategy and should therefore be specific to the company.

Stakeholder engagement

Suggestions in the area of shareholder stewardship and control include:

- Focus on strategic rationale for remuneration structures and involve both investment and governance perspectives.
- NEDs to serve on the Remuneration Committee for at least a year before becoming Chair.
- Shareholder representation.
- Employee representation on a Shareholder Committee.
- Annual binding shareholder votes on actual pay awards.

Investors have a responsibility to engage with the companies they are investing in. Although their views are generally on their websites, the challenge is in their implementation. Sometimes investors use a pay vote to signify dissatisfaction with something else. Communication is key and the remuneration report should be used to tell the whole story.

There are several possible approaches the UK could adopt to the shareholder binding vote:

- on the implementation report
- on incentive outcomes in the year
- the escalation approach, as described above, after two years of poor advisory votes
- special measures binding regime.

Similarly, different potential approaches exist to employee representation:

- employees on Boards/Remuneration Committees
- Shareholder Committees (e.g. the Swedish model)
- block-holder encouragement
- stewardship obligations or levy.

Fairness

This relates to the perception of the excessive quantum of executive pay and the differential between executive and all-employee pay. Suggestions for addressing this include:

- Introduction of mandatory publication of CEO to median worker pay ratios.
- Remuneration Committees should guard against the potential inflationary impact of market data.
- Annual bonus level should be reduced with 200% or more of salary only appropriate for the largest global companies.
- Publication of total cap on pay.

To take account of fairness, in 2017 companies could think about:

- justifying executive pay, through clear disclosure and open dialogue with shareholders
- introducing a fair pay charter with principles of pay fairness and explanation of pay policy
- disclosing a pay ratio.

Mandatory pay ratios are coming but the challenge will be how to make them meaningful.

Looking forward to 2017 and 2018 AGMs

The final messages for Remuneration Committees in order to build trust in a changing environment are:

- ***Transparency*** – Remuneration Committees need to be tougher on targets and assessments.
- ***Strategic alignment and flexibility*** – shareholders need to encourage the development of new pay models.
- ***Stakeholder engagement*** – shareholders should come together to exercise their existing rights decisively.
- ***Fairness*** – companies should set out their approach to fairness in a fair pay charter.

1/3

less on average is what the public think CEOs should be paid

Audit Committee update

The Audit Committee Network holds technical workshops three times a year which cover a regulatory briefing, a corporate governance and reporting update and an accounting development update.

At the most recent workshops, there was also a look at user access management.

PwC experts:

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

Iain Selfridge
iain.selfridge@pwc.com

Peter Hogarth
peter.hogarth@pwc.com

Dave Walters
dave.walters@pwc.com

Jessica Taurae
jessica.taurae@pwc.com

John Patterson
john.t.patterson@pwc.com

Iain Robinson
iain.robinson@pwc.com

Phillip Paterson
phillip.e.paterson@pwc.com

The first session began with a corporate reporting update. With little regulatory change the focus was on highlighting emerging trends/good practices, appreciating that what is good now will become common practice in two to three years' time.

The basis for the discussion was our annual review of reporting practices in the FTSE 350 and the work the corporate reporting team do in shortlisting companies for the 'Strategic Reporting' and 'Excellence in Reporting' awards at the annual Building Public Trust Awards.

Overall companies' strategic reporting continues to evolve rather than change dramatically. In the last year there has been an improvement in the quality of risk and governance reporting – presenting a more dynamic and integrated narrative that focuses on how risks are changing or what a Board has actually done in the year. This is in part due to the introduction of the 2014 Corporate Governance Code and the requirements for a robust assessment of risk and a viability statement. Looking further back there has also been an improvement in the quality of strategic reporting – how the strategy is increasingly used to underpin the strategic report and link to other key components such as business model, risks and KPIs.

The rest of the session focused on the three reporting challenges that are fundamental if corporate reporting is to remain relevant for business in the 21st century. For each challenge the findings from our work were presented supported by good practice examples. These challenges are:

Being distinctive

Greater individuality is needed in corporate reporting. There is a natural inclination at the start of the reporting cycle to dust off the annual report and consider what needs to be added – rather than starting from scratch to consider what needs to be reported. Similarly, an unintended consequence of the drive to adopt good practices is that many reports in the FTSE 350 are starting to look and feel the same with high level, often boiler-plate language. Too often companies present generic risks that could apply to any organisations or make references to 'competitive advantages' or 'distinctive capabilities' when discussing their business model without backing them up.

The Financial Reporting Council (FRC) in their year end reminders to CFOs and AC Chairs also picked this up with a request for disclosures to be specific and relevant to the organisation and its industry.

Being strategic

Despite the improvement noted earlier in the reporting around strategy, company reporting still falls short in how strategy is integrated through the disclosure and whether a forward-looking orientation is presented:

- Integration – only 40% of the FTSE 350 align KPIs with their strategy; 35% link risks to their strategy and only 1% align their market data to strategy.
- Forward-looking - 98% of FTSE 350 companies based their viability period on their strategic/business plans with the majority using 3 years for the period. However, only 11% of FTSE 350 companies appear to discuss strategy beyond the next 12 months.

There are two challenges:

- firstly, to try and map strategic priorities to the business model, risks and KPIs – where there are gaps can these be explained?
- secondly, is the strategy presented reflective of the one used for strategic planning or a simple point in time?

Being relevant

There was a debate around how reporting needs to adapt and evolve to reflect the dependency a company has on key stakeholders, their expectations, and the impact – positive and negative – on them. This will require companies to explain why these relationships matter, what impact they have on financial performance, how they are managed, and ultimately, to report new ways of measuring success.

PwC's 2016 Global CEO and Investor survey found that 63% of investors and 76% of CEOs said business success in the 21st century will be defined by more than financial profit.

Closer to home this trend/challenge can be demonstrated by how business models have evolved since the requirement was introduced three years ago.

- Over 50% of these disclosures now identify the key resources/relationships – either owned, or 'borrowed'.
- However, only 17% of companies align their business model and strategic objectives.
- Only 14% clearly link the business model with their KPIs.

A shift to a more stakeholder-orientated model may take time to get the right information and performance metrics but it is a task that needs to be started sooner rather than later.

Emerging themes

Finally, other areas of focus from the FRC year end reminders letter to CFOs and AC Chairs were considered – in particular, climate change, cyber security and Brexit risks. The discussion focused on how:

- reference to these risks might lead to excessive clutter and boiler-plate disclosure
- companies should be clear whether any of them (or others) are a risk, or not, to avoid undue misunderstandings
- ultimately companies should not allow boiler-plate disclosures to undermine the quality of discussion/processes and the confidence of management/Boards

Accounting update

The next session focussed on recent accounting developments – first with an update on FRC Corporate Reporting Review Team (CRRT) activity and an overview of their priorities.

In the past year, the CRRT looked at the annual reports of around 200 companies and, as is typical, wrote to about one third of them to explore areas of their reporting. The FRC has also been consulting on CRRT's operating procedures for reviewing company reports.

It is likely that the revised procedures will result in greater transparency regarding which companies have been reviewed and the issues that were raised.

The two thirds of companies whose accounts are reviewed but who do not know will, in future, be informed that the CRRT did not identify any substantive issues. Revised guidance for Audit Committees, issued in April 2016, will require AC Chairs to report on interactions with the CRRT.

The FRC's annual Corporate Reporting Review, issued in October 2016, identifies the following areas on which the CRRT will focus in 2016/17:

Strategic report: the remit is to ensure that reports are fair, balanced and understandable.

Clear and concise: Audit Committees should be identifying disclosures which are too detailed and should instead focus on materiality.

Accounting policies: the CRRT are looking for companies to be clear on revenue streams, and the specific accounting policies for each.

Looking ahead, with IFRSs 9, 15 and 16 coming into force in 2018/2019, the CRRT expects to see an increasing amount of information about what those standards will mean for a company.

Judgements and estimates: IAS 1 requires the disclosure of judgements and estimates. The CRRT is challenging Boards on the exact nature of their company's critical judgements.

Pensions: more transparency is needed in the impact of low interest rates on pension scheme liabilities.

Tax: the FRC performed a tax thematic review in the summer of 2016. The headlines from that exercise are:

- most companies responded positively
- there was evidence of discussion of tax matters in their strategic report
- reconciliations of effective tax rates were included.

However:

- less than one third of companies talked clearly about uncertain tax positions
- there was a lack of clarity around policies, judgements and estimates.

For 2016/2017, the CRRT priority sectors include:

- extractive companies
- companies servicing the extractive industries
- companies serving the public sector
- media.

If you are an AC Chair/Board member of one of these companies, there is an increased risk that you might be reviewed by the CRRT. Nonetheless, they aim to look at all FTSE 350 companies on a cyclical basis.

Amendments to IFRSs effective in 2016

The following is a breakdown of IFRS amendments to be aware of:

Standard	*Nature of amendment*
Amendments to IFRS 11	Acquisition of interests
Amendments to IFRS 10 and IAS 28	Consolidation exemption and sale/contribution of an asset
IASs 16 and 41	Bearer plants
IASs 16 and 38	Methods of depreciation
IAS 1	'Disclosure initiative'
IFRS 10 and IAS 28	Investment entities
Annual improvements	Various

As well as IFRS amendments, we also covered ESMA guidelines on Alternative Performance Measures (APMs) which is a focus for the CRRT over the next 18 months. The guidelines came into force on 1 July 2016. Issuers must:

- define the chosen APMs clearly
- reconcile back to the nearest GAAP number
- explain the purpose
- not display APMs with more prominence than GAAP measures
- present comparatives
- define consistently year on year and if making changes, explain why.

Prior to the ESMA guidance being applied, PwC conducted a survey and found the following observations from the FTSE 100:

- 95% of companies use an APM.
- 93% showed a reconciliation.
- <38% had the reconciliation on the face of the financials.
- <43% had the reconciliation in the front half.
- 4% did not present a reconciliation.
- 54% presented it in the notes.
- Seven presented reconciliations in other areas.
- Some even had separate non-GAAP sections at the end of their report.
- Total GAAP profit measure was £119bn and the total APM was £187.1bn giving a net upward adjustment of £68.1bn.

Regulatory update

The following session looked at the regulatory changes arising from the EU Audit Regulation & Directive ('ARD') for the Audit Committees of EU Public Interest Entities. This was timely as many Audit Committees are currently updating their terms of reference and auditor independence policies ahead of the start of the first year to which the changes apply (so from 1 January 2017 for a December year end company).

The session explained:

- how the ARD has been implemented in the UK by the FCA, PRA, and FRC
- the basic legal requirements for Audit Committees from the Directive, which are set out in the FCA Handbook and PRA Rulebook
- how the FRC has added to the basic requirements.

We also looked at how the Competition & Markets Authority Order ('the CMA Order') on the statutory audit market deals with the same areas, and includes a number of more specific requirements for FTSE 350 companies.

The key points arising were:

Sectoral competence

The Audit Committees of all EU PIEs will need, as a whole, to have competence in the sector in which the company operates. Participants debated how this requirement is being addressed in practice, which is a matter for case-by-case judgement.

Approval and pre-approval of non-audit services

The use of 'pre-approval' (whereby the Audit Committee has set a policy that individual engagements relating to certain services do not need any specific approval because of their nature or the size of the fee) has been limited by the FRC in its 'Guidance on Audit Committees' to those that are deemed by the Committee to be 'clearly trivial'.

This has resulted in the attention of many Committees being focused on two matters:

1) how to define and set a quantitative threshold for 'clearly trivial' and

2) whether the process of approving non-audit service engagements on a case-by-case basis needs to change because the use of pre-approval is now much more restricted (which will depend on the extent to which pre-approval has been used in the past).

NEDs shared their views on appropriate thresholds, which varied significantly - some related the choice to the quantum of the audit fee, while others did not.

The key issue in relation to the non-audit service approval process was identified as the extent to which Committees are entitled (and choose) to delegate their responsibilities to approve services in advance.

This is an area that requires some care, particularly in the case of FTSE 350 companies where delegation is restricted under the CMA Order to the Chairman of the Audit Committee (although the CMA Order does not restrict the use of pre-approval to services that are deemed to be clearly trivial). NEDs were reminded that all services that are not directly part of the statutory audit are non-audit services, including reviews of interim results – there is no exemption for 'audit-related services' in this case. It was noted that some Committees will now approve (on a case-by-case basis) all known specific non-audit service engagements at the start of the relevant financial year.

The session ended with a brief indication of the changes to auditor reporting that are being brought about by a combination of the EU ARD, the EU Accounting Directive and the IAASB's revision to international auditing standards. For the most part the changes are not fundamental for companies that are already used to long-form audit reports. However, the definition of a quoted company used by the IAASB means that companies registered on AIM will now also be the subject of long-form reports from their auditors on a mandatory basis.

The channels that apply to different types of EU PIE.

	PRA Rulebook (Banks and insurers)	FCA (Disclosure and Transparency Rules	UK Corporate Governance Code and FRC guidance	Competition and Markets Authority Order
Unlisted PIE (Banks and insurers)	✓	✗	✗	✗
Standard listed company	✓	✓	✗	✗
Non FTSE 350 premium listed company	✓	✓	✓	✗
FTSE 350 company (UK incorporated)	✓	✓	✓	✓

User access management

The last session focussed on user access management. Four common areas of interest are:

- clarity around who should own the process
- how to reduce cost around the process
- how to manage user identities across the organisation
- accessing the different levels of risk of access management.

Under the traditional IT model, employees used traditional applications on PCs accessed in the office, through closed corporate networks, with a small number of internal IT specialists having access to the underlying data and operating systems. However, due to a number of factors, including emerging technologies such as 'the Cloud', increasing use of third parties with direct access to company networks and the need to access applications whilst on the move, the risk landscape has now evolved. A number of different failures arise, mainly:

- former employees not being removed in a timely manner
- incomplete identification of users subject to review
- privileged access assigned to users who do not need it (or no longer need increased access).

These failures mainly derive from three different root causes:

1. ***Technical complexity*** – companies have a high number of systems and different platforms and technologies, yet there are system limitations and can be a lack of technical knowledge.
2. ***People*** – companies see a high turnover in staff, a lack of accountability between different departments and staff and contractors and third parties not being well monitored.
3. ***Processes*** – there are fragmented processes that are different across applications, a lack of governance, and controls not embedded early in the development phase of system and process changes.

However, there are a number of mitigating activities that fundamentally come back to ensuring the basics are done right and that means end to end controls throughout the access lifecycle. These cover:

- ***Security Settings*** – passwords to applications and security configurations are set in an effective manner.
- ***Joiners*** – access requests to the application are properly reviewed and authorised by management.
- ***Leavers*** – terminated application user rights are removed on a timely basis.
- ***User Access Review*** – access rights to applications are periodically monitored for appropriateness. Regular management review is performed of all accounts and related privileges.
- ***Privileged Users Monitoring*** – super-user/administrative application transactions or activities and sensitive generic IDs are monitored.
- ***Segregation of duties*** – policies are maintained for segregation of duties and are monitored.
- ***Traceability*** – all users and their activity on IT systems are uniquely identifiable.
- ***Logging*** – an audit trail is maintained of
  - direct changes to data
  - access of super-users
  - changes to configuration
  - sensitive access.

Looking to the future, continued evolution of technology will play a significant role in the area of user access management with a challenge posed as to how far advanced company thinking is around the impact and effective use. These include:

- Continuous Controls Monitoring (CCM)
- robotics
- cloud solutions
- risk based control solutions.

Some key questions NEDs can ask their CFO or CIO include:

- What access risks does the organisation currently carry and how are they being managed?
- Are there any user access projects underway and what are the objectives?
- What are the extent, severity and route cause of any access issues?
- Does the company's IT and information security strategy include consideration of user access management?
- Who has sensitive/ privileged levels of access and how is it managed?
- Has an appropriate evaluation been performed to mitigate the financial reporting risks of any access issues?

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

170120-160250-LS-UK