www.pwc.co.uk

Board discussions
What NEDs have been debating

September 2017

pwc

Contents

Introduction

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

The season began with our March briefings on **A global economic update.** These are uncertain economic times both in the UK and globally. At the global level, economic power is shifting away from the established advanced economies in North America, Western Europe and Japan where growth rates have been disappointing. China is now challenging the US to become the largest economy in the world and the Asia-Pacific region accounts for around a third of global GDP.

An early evening panel discussion in April moved from macro to micro and explored **Finance function effectiveness.** This was an event in conjunction with CIMA and the panel consisted of a listed company CEO, the CFO of a major private business and two senior representatives from CIMA. Discussions covered the challenges facing the finance function as it responds to the need to be a trusted business partner within companies. The session also explored how the role of the finance function might change going forward.

Our May lunchtime briefings looked at **The application of social media in business**. When used well, social media can be a powerful stakeholder engagement/ marketing and communication tool. However, the reputational risks associated with it are not insignificant as a number of organisations have found to their cost. The briefings covered key Board considerations in relation to an organisation's social media strategy, as well as a social media governance framework to manage the related risk.

Risk remains a constant feature of the Board agenda more broadly and we continue to focus on different aspects of this topic. Our summer workshop season included sessions considering **Risk management good practice including business control in overseas entities**. Companies and their Boards continue to be surprised by 'bad news' in overseas operations and today's global and interconnected business models mean that the inherent risk in this area is increasing. The workshops reflected on how to prevent breakdowns in control in overseas entities and how to rapidly detect issues when things go wrong.

As one specific area of risk, **Cyber security** was focused on in two separate workshops. The first covered the broad landscape of cyber security basics – setting context, explaining why this is a Board issue and providing a framework to help NEDs think about the key areas. The second explored seven principles for cyber security governance as well as a deeper dive into four key areas – developing a business perspective, assessing current state, improvement recipes and handling incidents and crises.

For when things do go wrong, the workshop season included 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 considered, and preferably rehearsed, plan swiftly into operation.

On a more positive note, another workshop explored **Strategic planning in a changing business environment**. In today's dynamic business world, strategy development needs to be an ongoing and deliberate process, governed by a rolling agenda of strategic issues and opportunities. The impact of disruptors should be considered but Boards should avoid lurching from strategy refresh to strategy refresh. Indeed, a well thought through long term strategy should make the decision-making in response to the disruptors easier.

The impact of disruption was further considered in our workshop looking at **Innovation for the earth – technology's role in solving sustainability challenges**. There is mounting scientific consensus that the earth's systems are under enormous stress. However, this is also an era of unprecedented technological advancement and the 4th Industrial Revolution (4IR) offers unparalleled opportunities to tackle environmental challenges. These were explored further in this workshop, alongside the need for a responsible technology approach to avoid social and other issues.

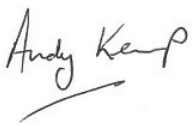
Our final workshop of the season looked at **Social media, digital tools and online hygiene for NEDs**. In contrast to the business application of social media covered in our May briefings, this session was from an individual perspective to help NEDs determine what type of online profile they might wish to have, since there is no way to avoid developing a digital footprint in today's world. The issue of 'online hygiene' to reduce exposure to breaches was also explored given that NEDs frequently sit on multiple Boards and sometimes work using their own technology.

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 sessions exploring treasury and the future of assurance.

For those on **Remuneration Committees** there were workshops looking at the continuing focus on executive pay by the Government, the media and the public at large. Proposed governance developments in this area were reviewed and there was a look at potential future requirements specifically in terms of executive pay policy, pay ratios, employee representation on Boards and fair pay disclosures.

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

We will continue to focus on matters featuring on Board agendas and look forward to further insightful discussions over the next six months of the programme.



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

A global economic update

These are uncertain economic times both in the UK and globally. At the global level, economic power is shifting away from the established advanced economies in North America, Western Europe and Japan where recent growth rates have been disappointing. China is now challenging the US to become the largest economy in the world. Other emerging market economies – like India, Mexico and Indonesia – are growing in economic importance. The Asia-Pacific region now accounts for around a third of world GDP and it is likely to continue to become increasingly influential through the first half of this century, as it is home to around 60% of the world's population.

At the same time, major political developments might change the shape of the leading economies in Europe and North America. In Europe, the shock of Brexit has raised questions about the future stability of the EU, as well as creating uncertainty about the outlook for key sectors in the UK economy which are dependent upon European markets. In the US, the Presidential election highlighted the frustration of many working people with a world shaped by globalisation.

Presenter:

Dr Andrew Sentance,
Senior Economic Adviser,
PwC – andrew.w.sentance@pwc.com

Global economic context

The session began with some context-setting around the post-crisis global economy. We are into the 8th year of economic recovery. It is a mature but not very strong recovery, hence the discontent that is being expressed in the political domain. Nevertheless, we are still in a growing global economy. World GDP will have tripled in value in US$ terms at current prices from US$33 trillion in 2000 to US$99 trillion forecast in 2021. In sterling terms, as the pound has weakened, the value is likely to have quadrupled from £20 trillion to £80 trillion.

The 'new normal' post the economic crisis is not far off the old normal of 3-3.5% per annum change in world real GDP. Global growth therefore remains close to the long-run trend. Inflation has been low but not deflationary as monetary policy decisions have headed off any risk of deflation. RPI is 3.5% versus a target of 2.5%.

However, what has become apparent is that there has been greater divergence of performance between countries, both in the West and among emerging markets. The US, the UK, Canada and Germany have all grown at 2% over the past seven years which can be considered good in the 'new normal'.

Italy, however, has contracted despite the global recovery which may be unprecedented. Greece has grown at less than 1% over a 35 year period which is not just down to the Euro but more due to structural problems with the Greek economy. Southern Europe generally has fared less well than the north due to a lack of reform of the labour market and being less business-friendly.

Outside of the West and Europe, some of the Far Eastern countries such as India and China have been growing at very healthy rates of 7-8%. The other BRIC countries of Brazil and Russia are very commodity-driven and have grown at 1-1.5%.

What is most noticeable is the rise of the Asia Pacific region. In the 1980s and 1990s, the West dominated with more than 60% of world GDP while Asia Pacific was around 20%. By 2030, however, the Asia Pacific economy will be larger than the whole of the West.

China is currently the 3rd largest economy at £11 trillion at current prices and market exchange rates but is expected to be the largest at £28 trillion by 2030. This is a significant point as the last time the largest economy changed was in the 1870s when the US overtook the UK. The big shifts in the global economy have already taken place and the US and China will remain the power houses.

US$99

trillion forecast world GDP by 2021

How have China, which has gone from a £500 billion economy to an £11 trillion economy in 20 years, and other countries such as India and Indonesia, made such progress? There are four key forces that have underpinned globalisation since the 1990s:

- Technology – which has brought the world closer together.
- Deregulation – particularly in Financial Services but in other sectors too.
- Political change – the collapse of the Soviet Union removed this as an alternative economic model.
- Trade liberalisation – with the single European market in 1993, NAFDA (the US equivalent) in 1994 and the World Trade Organisation in 1995.

Trade liberalisation in particular has been crucial to the development of the global economy with more than 95% of the world's population now living in a WTO member country.

There are four recent and prospective future phases of globalisation:

- 1993-2007 – Global economic boom supported by falling prices of manufactured goods ('the China effect') with easy money and strong confidence.
- 2008-2015 – Global financial crisis and its aftermath with weak productivity growth and real wage squeeze.
- 2016-early 2020s – Political fall-out (Brexit, Trump and anti-globalisation backlash) following disappointment of ongoing wage squeeze.
- Early/mid 20s onwards – Either adjustment and acceptance of a new more stable economic order or continued global political and economic conflict and volatility.

The first era of globalisation in the second half of the 19th Century was followed by very difficult times from 1914 to the late 1940s – 2 World Wars and extremely hard times in the 1920s and 1930s. This reflects the way in which a globalised world economy can break down due to conflicting national interests and protectionist pressures. A breakdown of the current globalised economic order is therefore a possible scenario but not the most likely outcome.

In the G7, Germany has been the best performer in terms of GDP per capita since 2000, followed by the UK but there has been a very slow increase in UK living standards. In Italy, GDP per capita is actually 5% below where it was in 2000.

Economic consequences of the UK leaving the EU

There are a number of economic consequences with different effects, principally:

- uncertainty associated with an economic shock (negative, short-term)
- disruption to trade and investment (negative, medium/long-term)
- restricted migration from EU (mixed)
- more regulatory freedom (positive, long-term)
- lower fiscal contribution (positive, but small).

PwC's view of the effect on UK GDP is a negative impact of between 1.5 and 5.5%. There is likely to be a negative net effect over a 10-15 year horizon, as predicted by most economic commentators before the vote, rather than a sudden 'falling off a cliff'.

The UK currently has a degree of momentum and is still close to the top of the G7 growth league. UK unemployment is among the lowest in the EU. Nevertheless, investment has dropped and sterling has fallen leading to a rise in import prices which squeezes consumers and offsets any positive impacts. Although the falls in investment and sterling are acting as a drag on the economy, they are not likely to lead to another recession.

Outlook

The 'new normal' is therefore still a growing world economy but a rate of 2% may now be considered good for the West. China, India and other Far Eastern countries are still benefitting from population growth and will therefore grow at higher rates.

c43%

of world GDP will come from Asia Pacific by 2030

Key implications for business and investment

- Global growth will continue in line with the 'new normal' trend but with divergences driven by economic fundamentals.
- Short-term growth prospects are improving – Asia, North America and Europe all growing quite well in 2017.
- Long-term risks are increasing – the US election result, Brexit and potential globalisation backlash add to global political and economic uncertainty and the risk of protectionism increasing.
- Brexit means slower growth and higher inflation in the short-term with longer term implications still uncertain.
- US and UK interest rates are likely to rise slowly to a 'new normal' level of 2-3% by the early 2020s with the Eurozone lagging behind.

In all these areas, therefore, a range of scenarios should be considered possible, especially for the medium/long-term outlook.

Open forum Q&A

The open forum Q&A was wide-ranging.

There was an enquiry about the impact of technology on the economic forecasts. Andrew is not of the view that unemployment will rise dramatically as technology could create as many jobs as it destroys. Technology supports productivity growth and improves the quality of life. Although technological developments are an important undercurrent in the jobs market, humans are very adaptable. 35% of the UK population used to be in manufacturing and now it is only 8% but the level of employment has remained similar. The challenge is more to policy makers to keep up with technology changes in terms of tax, pensions changes, etc.

Another NED wanted to explore the technology/productivity point further. It was noted that the UK's predictions are based on a conservative view of productivity, as monetary policies may have had some impact on this. Productivity has been dented by various 'shocks', including energy, financial elements and economic policy, but productivity also slows in a more service oriented model. 1-1.5% productivity growth may be as good as it gets going forward. There needs to be better focus on skills, infrastructure and tax reforms although politicians are sometimes reluctant to use these levers.

One NED asked about the future of the Eurozone which is caught up in the future of the European Union (EU). The EU is unlikely to collapse and Brexit may bring the remaining 27 countries closer. These countries together still have weight on the world economic stage. The Eurozone has adapted over time and the European economy is picking up.

Related to this a NED asked whether, if the UK were to take a 'hard Brexit' route with no satisfactory deal done, this would affect the economic projections. A 'hard Brexit' would probably mean a lower GDP. Looking ahead to 2020, there will be short term disruption but it will be in the interests of the UK and our trading partners to a secure a good deal.

Another NED enquired how the UK view would change if Scotland gains independence. More than 90% of UK GDP is in England and Wales and there could actually be some economic benefits if Scotland goes its own way. However, currency and the fiscal deficit would be big issues for Scotland as they would not be able to keep the pound and Scotland probably needs a better economic story. From a Scottish point of view, the potential attraction of being part of the EU with lots of smaller countries may be understandable versus an uneven economic relationship with England. Northern Ireland could also be interesting to watch with the unionist majority decreasing.

Following on from this, a NED wondered if an independent Scotland would look more like Greece or Ireland. Small economies are more manageable and therefore flexible. Finances from the UK would obviously be affected but Scotland could be left with a flexible economy.

A NED asked if the growing Irish economy is down to the corporate tax rate. Ireland effectively has a 2-tier economy: they have low taxation and a well-skilled work force. While the domestic economy has not been doing well, overseas investment has improved.

NEDs also wondered what will happen if we hit 2-3% interest rates. 2-3% is not particularly high compared to previous rates. The expectation is that we should remain at 0.2% but the UK will have to follow the international trend. The pace of increase and the way an interest rate rise is communicated has an economic impact. If it is communicated to the public properly and is a gradual rise, there should be no cause for alarm.

Another NED enquired about the relevance of balance of payment surplus/deficits. These are a feature of an integrated world and should not be used for political purposes. The US has a big deficit and Germany a large surplus but most of the others are relatively small. Arguably a country with a deficit is 'better' off as it consumes more than it produces.

Related to this, a NED noted that Government borrowing has increased and asked whether rising global debt will have an impact on interest rates. Globally, however, there is a good record of keeping the deficit low.

Looking further afield, a NED asked what the impact of a bad trade relationship between the US and China would be. It is not in China's interests to decrease trade with the US. Since the WTO has been set up, China has grown to an £11 trillion economy. Europe can play an important role as it has a strong trading relationship with Asia although this is more vulnerable than previously. A NED asked if the 'trauma' of the US being overtaken as the leading world economy was overstated. The US does still have a better standard of living than China but this challenge to being the undisputed economic leader for 150 years could lead to a political response.

Another NED asked if Trump is a true disruptor or whether he will be 'ground down'. The likely scenario is that he will be restrained. So far, we have seen no real progress with his agenda – his immigration proposals have not been accepted by the federal government and his economic agenda has not yet been accepted by Congress. He will continue to state his agenda but this does not mean it will come into force. If the US were to go down the protectionist route, this would negatively affect the global economy.

One NED enquired about the global effect of ISIS/the Islamic State. If the instability in the Middle East is contained, it will remain an issue for the Middle East. Oil prices may be affected but the oil economies are not the big players globally.

Following on from this, a NED asked where Africa and the Middle East feature in the demographic effects of a post Brexit world. The Middle East has natural resources but no large populations. If you looked below the top 20 economies, Saudi Arabia and Nigeria would be in the list. The African countries will be rising but not on the same scale as more developed economies as they are dependent on commodities, politically unstable and have low living standards. Nigeria and Ethiopia both have populations around the 100 million mark but living standards are still very low. To date, there are no strong African models that have worked.

Finally a NED asked how Greece can continue to survive based on its level of debt. Greece has some long-term problems which were evident before the introduction of the Euro. They might choose to leave the EU but this would not help them as their issues are more deeply rooted. The Greek economy might actually grow this year but it is a small part of the Eurozone.

No 1

economy will be China by 2030

Finance function effectiveness

In leading an organisation for the long term, a Board needs to consider the strategic direction in which the company is heading and the related decisions it needs to make. Today's finance function is transforming to play a greater role in supporting this critical decision-making process. The remit of effective finance functions now covers areas such as:

- ***security***
- ***control***
- ***strategic direction***
- ***ownership of the business model framework.***

The finance function is increasingly responsible for accounting for the business as a whole, and not just the balance sheet, with greater emphasis on non-financial metrics.

CIMA is leading on research to enable Boards to assess the effectiveness of the finance function to drive performance and success for the short, medium, and long term. This includes the quality of the information received to support good decision-making and governance

Panellists:

Ian King – CEO, BAE Systems Plc

Ian Bull – CFO, Parkdean Resorts

Charles Tilley, OBE – Executive Chairman, CGMA Research Foundation

Dr Noel Tagoe – Executive Vice President: Academics, CIMA

Context and the Board perspective

Charles opened the session noting that CIMA, with AICPA (the American Institute), had recently formed the Association of International Certified Professional Accountants strengthening their combined resources to better support their combined membership to keep up to date and relevant.

Charles is the Chair of the International Federation of Accountants and the focus at their recent half-yearly meeting was on maintaining the relevance of accountants and the finance function so the subject under discussion is topical. Questions to be considered include:

- What do businesses need from their finance function now?
- Has accountancy developed sufficiently to meet today's needs, taking into account technology and other developments?
- Is the right information provided to enable businesses to take decisions focused on the long-term sustainability of the company?

The business environment is changing rapidly and finance functions must consider what they need to do to keep up. The core roles of security, control, strategic direction and ownership of the business model framework are fundamental, underpinned by integrity, confidence in the numbers and being a trusted business partner and commentator.

The finance function, as co-pilot of the business, needs to ask, 'How are we going to get from where we are today to where we want to be tomorrow safely?' and then assist with this process.

Technology and the widening role of business are also driving how the finance function needs to change. There is a need to respond to a greater range of stakeholders. Only recently the CEO of the Brazilian bank Itau Unibanco, (an organisation larger than Barclays), spoke about needing to create value for shareholders, employees, clients and society. Often the majority of this value is not recorded on the balance sheet resulting in the need for more non-financial metrics. This is proving to be a challenge with strategic reporting further putting a spotlight on these.

Charles referred to CIMA's recent 'Joining the dots' publication which looks at how companies are struggling to be agile, take a long-term view and have the right metrics and skills. In a survey of more than 300 executives globally, it was noted that:

- 72% had a strategic initiative fail due to delays in decision-making.
- 80% had based decisions on flawed information.

The finance function needs to be the owner of the business model framework (not just the numbers and the balance sheet) and the link to systems, processes, risk analysis, remuneration structures and values.

As a result of this central role of the finance function, there is a case for Boards to assess the effectiveness of their finance functions just as Boards themselves are subject to effectiveness reviews. Charles referred to a PwC survey which, in 2010, suggested only 11% of finance functions were rising to the challenge, a statistic which had only increased to 45% by 2015. CIMA have developed a diagnostic to assist in exploring 'what good looks like for the finance function'.

Perspective of a CEO

Ian King noted that BAE Systems is an amalgam of long-term contracting in defence and security with a huge geographic spread. They therefore need a set of core processes that are consistently tailorable across all areas and geographies, particularly in terms of how they manage projects, how they manage people, performance management, etc.

There is no meeting that the finance function could not ask to attend. Long-term contracts have risks that are not linear and the finance function needs to understand the dynamics of a project and therefore be a genuine business partner. The challenge is 'how far you get into the pond'.

The finance function is in a privileged position but needs to be a genuine business partner in order to be able to form a view. If there are errors, both the MD of the relevant business and the FD will be equally accountable as they need to be working in tandem.

As a CEO, Ian looks for integrity and authority in his finance function. He would not expect them to be sitting on their hands if something is going wrong but actively following up. The high visibility and access accorded to the finance function are accompanied by high expectations. These are made clear to individuals pre-appointment, including Ian speaking to them directly, and targets are owned and explained to the Audit Committee and Remuneration Committee.

72%

of companies have had at least one strategic initiative fail due to delays in decision-making

A couple of challenges that Ian feels their finance function faces are:

- Whether controls are testing how they previously managed the business or how it is currently managed (particularly in view of ongoing automation).
- The fundamental changes that IFRS 15 will bring in terms of working out profit on contracts against the cost profile. The Audit Committee will need to agree to upcoming changes in this area and there will also be market and customer expectations to take into account.

Perspective of a CFO

Ian Bull noted that Parkdean Resorts is a large private business running holiday parks across the UK. It merged in 2016, was sold by the end of that year and would be a FTSE 250 company if listed. Its ambition is to 'grow in all the right places and build a fabulous, sustainable business'.

In Ian's experience, the Board seeks six main things from its finance function:

- confidence that all the bases are covered
- reporting – both the basics and additional KPIs
- risk assessment and management
- data analytics
- IT
- support with the people agenda.

The finance function needs to ensure this is all joined up.

Reporting of the basics needs to be good and slick. Ian's aim is to get management reporting done by day 2 (currently this is day 5) and audited annual accounts by the end of January. These need to be right but getting them done quickly will free up time to focus on the more interesting, value-adding elements.

In order to be able to add value, finance function personnel need to understand the business and the drivers and predictors of performance so that they can provide user-friendly dashboards.

Risk assessment and management is crucial. The finance function needs to be aware of what can be controlled and what cannot and ensure there are good early warning systems in place. Reputation risk is particularly important as people will not rebook a holiday if they have a bad experience and may also put others off. The finance function can provide a heat map of what good looks like but it is the executives' job to bring it to life.

Data management is also very important, even more so as Parkdean is a regulated business. Data analytics can be defensive – looking at security, safety and cyber which is a constant process and includes the organisation employing its own ethical attackers. However, it can also be offensive – using analytics to uncover trends, challenge the business and understand the life-cycle of the customer. The various systems also need to be looked at not just from a control perspective but also in terms of service enhancement, such as reducing queues.

IT needs effective governance and Parkdean look to adopt best practice from the plc world.

The finance function also needs to co-develop the strategy with regard to people development. Acting as a co-pilot, they may disagree with the pilot occasionally in private but never in public. They need to put plans together jointly and be jointly accountable for successes and failures.

All of the above needs a finance function with strong capabilities and also one that understands benchmarks and is prepared to make tough decisions and recommendations when necessary.

Using CIMA's research to bring this all together

To summarise Noel focused on three key areas:

- measures to check whether a finance function is effective
- the principles underpinning these
- what the future looks like for the finance function.

Measures

There are six key types of measure that can be explored in assessing the effectiveness of the finance function:

- coverage and scope of the finance function
- cycle time
- cost measures (how much it costs the finance function to operate)
- quality measures (e.g. errors, auditor views, etc.)
- relational (what is the quality of relationships internally and externally with stakeholders)
- outcome measures – financial performance
  - for stakeholders (e.g. as NEDs, is the finance function giving us what we need?)
  - helping the organisation to position itself in its environment which requires innovation, resilience and agility.

Principles

The four key principles underlying these measures are to:

- communicate insightfully
- provide relevant information (not just what but when and how)
- explain how value is created
- report with integrity to engender trust.

80%

of executives surveyed say their organisation has used flawed information to make a strategic decision

Future

The future will be:

- the same in terms of needing to collect information, analyse, incite to act and measure, although how this will be done will change
- broader, as the finance function continues to move beyond numbers to truly supporting the business model
- digital.

Open forum Q&A

The open forum Q&A was wide-ranging and addressed a number of areas.

One attendee asked the panel how they would expect a NED to challenge a CFO/finance department based on a presentation to the Board. The key is to not just rely on these set meetings. The AC Chair should build a relationship with the CFO offline so that there is always the opportunity for phone calls outside of meetings. As well as being an executive, the CFO is a member of the Board and should be prepared to present an alternative view/stand up to the CEO when necessary. The NEDs can also ask the finance function what they can do to make it more effective and can be clearer about what the Board needs.

Another NED asked whether the increasing sophistication of data analytics is likely to reduce or increase the value of the finance function. This is a developing area and the ability to connect financial and non-financial metrics is key. There will sometimes be a need to combine finance function data with external source data.

CIMA's research to date seems to indicate that data analytics is not undermining the role of the finance function but different skills may be needed. There may also need to be a shift in mindset from right and wrong to 'looks about right' whilst maintaining integrity and one version of the truth. Greater agility will be needed to get the information required quickly from whatever is the best source.

Another attendee enquired about the clichéd view of the CFO as negative, secretive and cynical, believing that control of the numbers gives him/her power. In this regard, he asked how CFOs will cope with the changes required to become a true business partner with a relevant voice. It was agreed that some of the more traditional skill sets will not be those of the future as the role becomes more about interpretation than number-crunching. Whilst the traits mentioned can sometimes be seen, there are many other CFOs who are valued for their views.

This will depend in part on recruiting people with the right collaborative mindset and will also come from how the leaders of the finance function behave. Some companies send CFOs out into the business to gain experience and further develop business acumen. The CIMA accountancy curriculum has also been developed to cover technical skills, business acumen, people skills and leadership skills, with the recognition that people will need this in varying ratios at different stages of their career. Expanding the curriculum also helps to attract the right people.

A final question was around the dynamic between the Chief Strategy Officer (CSO) and the CFO, whilst also noting that if the CEO and CFO both have a financial background, a company can end up with two first officers rather than a pilot and co-pilot. The Board has ownership of the strategy but it is delivered through the executives via the CEO and therefore the CSO still needs to report to the CEO. There can be tensions between the CFO and the CSO but the CEO needs to be able to direct this appropriately.

70%

say there is room for improving collaboration between leaders and employees

The application of social media in business

When used well, social media can be a powerful tool for use in business. Its use is also expected by 'millennials' and subsequent generations who increasingly represent the majority of the workforce and customer base. However, the reputational risks associated with social media are not insignificant.

The session sought to explore key Board considerations in relation to an organisation's social media strategy and the Board's role in managing the related risks.

Presenter:

Phil Mennie, Global social media and governance leader, PwC – philip.s.mennie@.pwc.com

Context

The session began with some context-setting around the definition of social media. People automatically think of applications such as Facebook and Twitter but social media is much broader than this. It also encompasses areas such as photos, videos, music, blogs, messaging, events, podcasts and file sharing. It is any digital platform that enables the sharing of data with multiple users, helping people to connect and communicate with one another.

Social media began about 11 years ago, initially within universities, but has proliferated since to encompass almost all aspects of everyday life. This was illustrated by the fact that the English Oxford Dictionary word of the year for 2015 was actually the emoji representing 'crying with laughter'. Today our lives are ruled by our smart phones which are often the first thing we check in the morning and the last thing we look at night.

The Chief Editor of the FT has described the hard copy paper as a complementary service since news breaks first on social media. Arguably the hard copy is already out of date when printed. As another example, fitness trackers have been brought to life by social media with individuals competing to share their successes.

There can, however, be unintended consequences of increased smart phone use. An individual's whereabouts can be identified via their phone's GPS location. There are also many instances of people's homes being burgled when social media posts have indicated that they are elsewhere.

2015

English Oxford Dictionary word of the year was an emoji

Risks of social media

A number of examples were talked through to illustrate the risks that can arise from careless/improper use of social media. These included:

- the Syrian Electronic Army, a hacktivist group, hacking The Associated Press in 2013 and stating that Barack Obama had been injured in explosions in the White House causing an immediate shock to the stock market
- geo-tagging of phones used to take photos of newly-delivered helicopters at a base in Iraq being used by the enemy to destroy them
- a PR guru tweeting an ill-informed joke regarding Aids leading her to be fired mid-air as she flew to Africa
- a betting winner taking a selfie with her winning ticket resulting in someone using the bar code to claim her winnings
- BP's handling of the Deepwater Horizon oil spill where a fake BP PR account set up to mock BP's reaction gained more followers than the official site
- British Gas offering a Twitter Q&A following a price rise and receiving critical responses – illustrating the importance of getting the timing right in social media
- ASK.fm being used for cyber bullying given the anonymity afforded and illustrating that there is no escape from the bullying as social media is always on
- inappropriate 'hijacking' of hash tags to publicise products
- mixing-up of personal and corporate Twitter accounts.

There was, however, an example where a potentially detrimental social media situation was handled well. When the Wikipedia entry for Greggs was hacked to include an offensive message about their products and customers, Greggs tweeted a photo of doughnuts asking Google to fix the problem. Google responded that if Greggs included some sausage rolls they would get on to it asap. Greggs' responses to individual members of the public who tweeted were also effective striking the right tone despite Greggs receiving 30-40 tweets a second at the height of the scandal.

30-40

tweets per second during the Greggs incident

Opportunities of social media

Outlining the risks should not give the impression that this is all too risky. Companies need to be embracing social media and not trying to shut it down. There can be huge opportunities if social media is used well and it is just a case of making sure there is rigour, control, strategy and purpose around this. Some of the benefits of social media include:

- better engagement with customers, employees and other stakeholders – being able to connect quickly and build advocates who may come to the rescue when things go wrong
- gaining competitive advantage
- more targeted and effective marketing – can target exactly customers most likely to buy specific products, although data must be used ethically
- better feedback from customers
- increased brand awareness
- improved customer service and satisfaction – especially where systems exist for tracking queries and getting them to the right people for a response
- increased loyalty and advocacy from customers
- higher employee productivity – e.g. via internal networks for collaboration.

Within PwC, there is an internal social media site that is used for collaboration and has 180,000 users. The average age of a PwC employee is 28 and the firm therefore needs to ensure it has technology and tools that this generation would expect to be able to use.

Social media governance framework

There are a number of elements to a good social media governance framework as follows:

Social media policy

- a policy that fits the culture of the organisation
- guidance on how to use the platform appropriately.

A company's social media policy should be short, not written in legalese and encourage the use of social media within defined parameters rather than instructing people not to do certain things. The policy also needs to be visible so that people know where it is.

Social governance framework with

- roles and responsibilities
- metrics
- metadata management.

Social media has often grown organically within a company, frequently starting in marketing and then spreading to customer services, HR, IT, risk and compliance, internal audit, sales, etc. This can mean that each department has created its own social media policy and may not be communicating with others to ensure these are joined up. The social media policy also needs to be aligned to the company's business strategy and match its values and culture. Roles and responsibilities need to be defined with consideration of whether any metrics used are appropriate and if the Board sees them.

Social resilience and crisis management including

- incident response planning
- platform resilience
- moderation/monitoring.

At some point, something probably will go wrong and it helps to have predetermined, and ideally rehearsed, who will take charge and make decisions. The initial incident may have nothing to do with social media but, once it moves into this domain, there can be a huge PR issue to deal with.

Regulatory/compliance such as

- eDiscovery
- client confidentiality
- legal implications.

The use of social media must be in compliance with laws and regulations such as the General Data Protection Regulation which will shortly be in force. In the US, the regulators have recently clamped down on organisations paying celebrities to say they like a particular product on social media which is effectively a form of sponsorship and needs to be clearly indicated as this to avoid fines.

Social strategy including

- adoption and growth strategy
- risk awareness.

The social media strategy needs to be integrated with the business strategy and not run as a separate 'add-on'.

Policy awareness and training via

- online training
- mentoring/coaching
- embedding policy and positive behaviours.

Training, which could be online, needs to raise people's awareness and increase their confidence in how to use social media. At PwC, a reverse mentoring scheme has operated where the younger generation have mentored senior partners in this area.

Data privacy and control encompassing

- IT security
- data retention
- EU Data Protection vs US eDiscovery.

Many social media accounts are hacked but there are controls that can be put in place to prevent this. For example, each Twitter account has only one password which has caused users to share passwords contravening good practice. It is, however, possible to have a management system sitting between the user and Twitter such that passwords are not shared. It may also be appropriate to have approval processes in place before a company's social media messages go out.

Key questions for NEDs

- Is there Board level awareness of both the opportunities and risks of social media?
- Does your company have a social media strategy?
- How is your company exploiting social media opportunities in comparison to your competitors?
- How do you ensure your social media activities are compliant with laws and regulations?

Open forum Q&A

The open forum Q&A was wide-ranging.

One NED asked whether there was any correlation between the growth of Facebook, Twitter, etc. and the stagnation of productivity. In fact, there are instances where internal collaboration systems can increase productivity. PwC's Spark system has enabled the easier identification of 'knowledge' owners/subject matter experts. Embracing social media and related technologies is important as their advancement is inevitable.

Another NED enquired whether excess screen time desensitises people or leads to short term memory being affected. There may be some truth in this, as has been argued in the case of violent video games, but there are also positive impacts.

There was a concern about the extent to which social media can influence and manipulate. It is definitely the case that people are most attuned to channels they relate to which can then reinforce their beliefs and effectively group like-minded people into 'belief bubbles'. Social media can also be used to influence, an example being when undecided voters were targeted during the Brexit campaign having been identified by posts on social media.

There were questions around where regulatory intervention should come from to protect consumers of social media without stifling innovation. Is this the responsibility of service providers or government? Service providers have a duty of care and should take a lead but there may be a role for government too. Government at least needs to understand the technologies in order to be able to legislate to protect citizens if necessary. However, the UK would not want to get to a point of censorship as exists in some countries. Having younger people advising, as well as understanding consumer sentiment in how people want to use technology, would be helpful. There is a also a degree of self-regulation to some extent where the public at large will complain/monitor.

Another NED noted that from a corporate point of view it can be good to build a strong and supportive social media community as they will often become advocates for the company when things go wrong. Another added that an organisation's employees are often a good proxy for the outside world and, in fact, may sometimes take a harsher view internally when issues arise.

Further questions were about who in a company should be responsible for setting social media strategy. In consumer based businesses, this is often the CMO but it can be the Head of Communications in a less consumer facing business. Whoever it is, the social media strategy needs to be integrated into the wider business strategy and consider questions such as 'how do we want to be perceived?' and 'who are we mostly targeting?'. Having working groups who come together to discuss this, plus involving younger people who can ensure the tone is right and is not just 'corporate speak', can work well. The social media strategy also has to have appropriate controls built in. Social media engagement is often done well in the public sector which is focused on serving the public and more comfortable with the idea of control in this space.

One NED noted that in FS it can be difficult to focus on the positive aspects of social media, partly because of the negative impacts of some advertising. Generally, advertising is accepted if it is relevant to the individual and there is plenty of data available to enable organisations to work this out. The FCA has produced some reasonably helpful guidance on advertising in social media.

There was a question around whether Boards should encourage senior teams to embrace social media. 'Encourage' is the appropriate word as it is unlikely to work if it is mandated. Having reverse mentors guiding senior individuals who want to engage with social media but do not know where to start has worked well at PwC.

Another NED asked how to tell when something trending on social media could tip into crisis management, i.e. when 'noise' starts to become something that is running out of control. There needs to be 24 hour monitoring of social media – not just during office hours – and there are companies that can provide this using a mixture of algorithms and people. Ideally crisis management needs to be practised so that people are clear about their responsibilities and who the decision-makers are. Social media is often the communication element of a crisis.

A NED asked for an international perspective and it was noted that social media is global. However, there may be different platforms in different territories and there can also be varying attitudes to the degree of freedom of speech depending on the country.

Finally, a question was asked about looking ahead and the future of social media. Live-streaming is currently becoming popular and there are likely to be new platforms. However, digital advancements more broadly will have greater relevance. Virtual reality, augmented reality and artificial intelligence are all likely to have significant implications for business. The question for organisations is who on the Board properly understands this.

Strategic planning in a changing business environment

The amount of time a Board spends on strategy has been rising but many NEDs would still like to devote more time to this area. In today's constantly changing environment, something more dynamic than the typical annual offsite strategy day may be needed. The executive management team's horizon has become shorter as they grapple with the latest disruptors. Boards, and particularly the NEDs who often have a longer tenure than the CEO, need to keep an eye on the longer term to ensure the organisation remains sustainable.

Strategic planning has become more challenging in today's dynamic environment and the workshop was an opportunity to explore the elements of a good strategy, what makes an effective strategic planning process and the role of NEDs within this.

PwC experts:

John Potter, partner at Strategy&, PwC's strategy consulting business – john.potter@pwc.com

Leo Johnson, partner at PwC and leader of PwC's disruption team – leo.f.johnson@pwc.com

Context

Strategy has been a concept in military circles for hundreds of years but business strategy only really began to emerge in the 1960s when companies grew in size. Since this time there have been 4 main schools of thought as follows:

- Positional – identify markets in which the company can dominate and build a portfolio of positions in this. Responds to 'where do you want to be as an organisation?'.
- Execution – the difference between companies with similar strategies flourishing or declining was thought to be in the execution so this led to an era of benchmarking which in turn created a degree of convergence.
- Adaptation – with the advent of the internet, the need to be agile grew in importance resulting in the generation of lots of ideas to find out which ones work but this led to a lack of focus and difficulty in deploying scarce resources.
- Concentration – a focus on core capabilities rather than products and markets.

50%

of CEOs don't think they have a winning strategy

From strategy to execution

A decade of research and insight into practices at leading companies led Strategy& to the identification of five fundamental principles for how to connect strategy to execution which are often the opposite of what companies traditionally do:

- Commit to an identity (rather than focusing on growth).
- Translate the strategic into the everyday (rather than pursuing functional excellence).
- Put your culture to work (rather than reorganising to drive change).
- Cut costs to grow stronger (rather than going lean across the board).
- Shape your future (rather than becoming agile and resilient).

Each of the five acts of unconventional leadership listed above was then explored in more detail.

1. Commit to an identity

Companies need to define who they are as a company and stay true to their value proposition and capabilities system over time. The company is defined based on what they do rather than what they sell. Committing to an identity means answering the questions – 'who do we serve?', 'how do we create value?', and 'what do we need to be really good at?'. In part, this identity is defined by a company's purpose and remaining true to it helps to define the brand.

This was illustrated by the example of Amazon that adds value for customers by creating a 'digital marketplace' that continually responds to its customers' changing needs.

In contrast, there has arguably been recent damage to the long-standing brand of a major airline by it not being clear about its identity, e.g. now trying to compete with low cost airlines.

2. Translate the strategic into the everyday

It is not enough to define the company's identity, companies need to translate it into the everyday. In order to do so, they need to blueprint and build their distinctive capabilities system and then bring it to scale across the entire enterprise.

IKEA was used as an illustration. The company was founded on the principle that everybody – not just wealthy people – should be able to buy furniture. In order to succeed in offering home furnishings at low prices, IKEA had to build a world-class capabilities system, including deep understanding of how customers live at home, efficient, scalable, and sustainable operations and customer-focused retail design. The fourth capability that makes them stand out is price-conscious and stylish product design. Their design systems are so detailed that the cost implications of every choice, e.g. changing from four colours to two, are built-in. Their flat pack concept also totally changed distribution costs.

3. Put your culture to work

Companies need to leverage and enhance the culture they have to develop and maintain coherence. Strong cultures feel very different and this was illustrated by Natura, the Brazilian cosmetics leader, which is a relationships focused experience provider and has built its reputation on connecting to nature.

4. Cut costs to grow stronger

Companies need to invest where their strategy is and free up resources to invest in their capabilities. Costs that do not directly support the strategy and capabilities should be cut.

Amazon's internal culture is very frugal except where expenditure is seen to ease friction for consumers. Even small items such as desks are difficult to get approved but the cost of five distribution centres in North America was passed easily because of the benefits to the customer.

5. Shape your future

Over time, focusing on what they do best allows the best-performing companies to develop capabilities that go beyond their original goals. They do not complain about the state of their industry — they reshape it.

There was some discussion around whether this framework was too inward-looking, as a company's focus needs to be on solving others' problems. Often time is the enemy of the NED in relation to strategy as insufficient discussion in the Boardroom focuses around:

- Who are the key stakeholders?
- What do they want right now?
- What will they want in 5 years' time?
- What are the disruptive factors that may come along?

Tapping into broader stakeholder views was briefly discussed and it was noted that B&Q had created a youth Board to feed into the main Board. Worker representation may also help with this in some instances.

Disruption

Megatrends – accelerating urbanisation, demographic, political and social change, resource scarcity and climate change, shift in global economic power – accompanied by rapid technological breakthroughs are causing significant amounts of disruption in business today.

As an illustration, a number of potential investment opportunities were briefly considered but all had potentially significant disruptors:

- Airports – 30% of life may be experienced through virtual reality by 2020 and 41% of cargo may be replaced by 3D printing.
- Utilities – high fixed costs, low margins, high volumes model may be disrupted by new technologies such as electric batteries.
- Motorway service stations – likely to be disrupted by driverless cars and electric vehicles.
- Crematorium – we may even ultimately solve dying as double the current life expectancy (to 160 years) could be a reality within 20 years as some of the key diseases are close to a cure.

The march of technology continues and Oxford University research estimated that 47% of white collar workers could lose their jobs by 2030. The timing and probability of disruption can be difficult to assess but businesses can:

- identify all the elements of their ecosystem
- work out which bits are critical to the business model
- consider what could disrupt these.

The world is moving into unchartered territory as disruptions are happening very quickly.

A framework considering scenarios of the future was explored. With huge amounts of innovation and decentralisation, we could potentially see the rise of the machine and cities built on algorithms no longer needing the influx of migration. High innovation and a more centralised approach could mean less jobs and risk from climate change leading to global rationing. Zones where businesses lose their licence to operate can lead to the survival of the fittest. However, there is optimism as society has a history of adapting. If intellectual property is distributed rather than the current centralised ownership model then business should be able to solve society's problems and get to a position of inclusive growth.

The NED role is to scan the horizon and look for signals indicating disruption. There can then be consideration of the relationship between the timing of these disruptors and core business model requirements. Often with hindsight there were warnings of 'black swan' events but the interpretation of data often excludes items that do not fit the strategy.

Instead of conventional metrics, NEDs should consider the following elements of an 'index of strategic agility':

- peripheral vision/focus on anomalies
- wild card framework
- external networks
- compelling hypotheses
- trigger points/threshold
- structured debate
- plural team
- scenario-based planning
- multiple competencies
- opportunity-driven investment.

9 out of 10

executives concede they are missing major opportunities in the market

What does disruption imply for the strategic planning process?

According to the UK Corporate Governance Code, NEDs have the key roles of:

- Strategic input – as part of their role as members of a unitary board, non-executive directors should constructively challenge and help develop proposals on strategy.
- Evaluation of strategic execution – non-executive directors should scrutinise the performance of management in meeting agreed goals and objectives and monitor the reporting of performance.

Key elements of an effective strategy setting process are:

- Strategy development must be an ongoing and deliberate process, governed by a rolling agenda of strategic issues and opportunities.
- The development of a strategy should differ from the development of a plan (e.g. actions, resources, performance targets set to meet the strategy).
- Strategy should be kept separate from important topics such as governance, compliance, finance and risk management.
- Board members should be included throughout the development, approval and executional review of the strategy.

Ongoing and deliberate means that a strategy should not be frequently changing course. The impact of disruptors should be considered but should not necessarily lead to a new strategy. Boards should avoid lurching from strategy refresh to strategy refresh as a well thought through long term strategy should make the decision-making in response to disruptors easier.

The business plan clearly needs to tie into the strategy but the two are not one and the same.

Time for strategy at Board meetings is often hijacked by other agenda items so separate periods for consideration are likely to be required.

NEDs should be involved in the active development of strategy throughout the process. It is not for management to develop strategy in isolation and the NEDs to then challenge it, although it is the executive team that is tasked with implementation.

NEDs can be actively involved in strategy development through the use of strategic intuition. They have 'collections of memories' possibly from outside of the sector or from things they have seen work elsewhere and also have the bandwidth to be able to step back. They should bring a diverse collection of experiences to the process. Scenario planning can also be a helpful tool.

The role of the Chairman is very important in the strategic planning process, as is the quality of the relationship with executive management. There is a natural tendency for the CEO to want to control the debate but the Chairman should encourage the leveraging of experience around the table. Often a defensive executive team and the asymmetry of information between the executives and non-executives can be a common starting point and the Chairman needs to create a good strategic planning process out of this. In practice, meetings in advance of Board meetings to 'chew the cud' are often a part of the process.

Undoubtedly more time on strategy is needed throughout the year and the Chairman needs to ensure strategy does not get crowded out. The Board should consider relevant issues, possibly using third parties to do some scenario planning around the disruptors. Different scenarios can be mapped out to look for any dominant or common themes and NEDs should also ensure that horizon scanning is happening within their organisations.

Conclusion

The session concluded with a number of questions NEDs could ask to assess whether their companies have a strategy that works:

- Commit to an identity
  - Are you clear about who you are as a company and how you choose to create value?
  - Would stakeholders – internal and external – give the same answer?
- Translate the strategic into the everyday
  - Have you specified how each distinctive capability works and how it helps to create value?
  - Do you have a plan for how to innovate and advance these capabilities over time?
- Put your culture to work
  - Do you consider your company culture something inherently positive?
  - Are you clear about how to leverage and scale up the positive aspects of your culture?
- Cut costs to grow stronger
  - Is the majority of your expense budget invested in your distinctive capabilities?
  - Do you have aggressive cost targets to reduce investment in non-critical areas?
- Shape your future
  - Do you have privileged access to customers so you can meet their needs better than others?
  - Are you driving change in the market and shaping your own future?

8%

of leaders excel at strategy and execution

Risk management good practice including business control in overseas entities

Companies and their Boards continue to be surprised by 'bad news' in overseas entities. As today's search for growth and reliance on ever more extended value chains often mean that companies are doing more in emerging markets, the inherent risk profile before controls are put in place is increasing.

Boards are grappling with how to prevent breakdowns in overseas operations as well as how to rapidly detect issues and minimise the damage when things do go wrong. The workshop was an opportunity to reflect on these areas.

PwC experts

Tracey Groves
tracey.groves@pwc.com

David Andersen
david.c.andersen@pwc.com

Simon Perry
simon.perry@pwc.com

James Maxwell
james.maxwell@pwc.com

James Smither
james.smither@pwc.com

This workshop began with a look at the context and why there needs to be a focus on overseas territories.

Context

Being global is no longer an option for many businesses today for any or all of the following reasons:

- the quest for growth, market share and untapped consumer populations
- lower cost labour
- tax efficiency
- control of key raw material inputs
- M&A activity that expands the corporate footprint
- supply chain optimisation
- emerging competition and market disruption
- technology enablement of global presence
- diversification and avoidance of dependency
- globalised clients expecting uniform service regardless of location.

However, control systems have often not kept pace with this expansion overseas. In their absence, the risks inherent in such locations can result in unwelcome headlines highlighting incidents of corruption or anti-competitive behaviour, cyber security breaches, tax disputes and accounting breakdowns.

As well as causing reputational damage and attracting regulatory scrutiny, these incidents can damage the share price and have significant detrimental impacts in terms of management time and staff morale.

The latest PwC CEO survey indicated that CEOs are looking at countries such as China, India, Brazil and Mexico to drive future growth. The risks in such markets are unlikely to dissipate, meaning a closer focus on how to manage them effectively will be required.

Understanding the challenge

Key drivers of the risk landscape in overseas territories include:

- Volatility – some countries are intrinsically more unpredictable or unstable.
- Stakeholder scrutiny – by regulators and enforcement agencies, shareholders, civil society organisations and host communities.
- Distance – physical separation of remote offices can inculcate a 'them and us' environment in which instructions are ignored or bad news buried.
- Complexity – a desire for common standards against a backdrop of highly complex and inter-dependent global business structures.
- Oversight – less visibility and control of joint ventures, non-operated subsidiaries or franchise models.
- Integration – legacy behavioural and third party relationship risks when overseas growth is by M&A.
- Culture – different ways of doing business or understanding of the values espoused by Head Office.
- Technology – knowledge of risk incidents in remote locations can be instantaneous and widespread.

Understanding this landscape and the significant variations between different overseas territories requires nuance and the need to assess the different risks in each location, meaning a 'one size fits all' approach to compliance will often not work. 'Eyes on the ground' are important in this respect and visits to territories by the NEDs can help increase both understanding and nuance.

Since the financial crisis, the amount of legislation and regulation spanning multiple compliance topics has also increased in all sectors and the reputational risk of a breach, or perceived breach, continues to grow.

Four months ago, the Ministry of Justice launched a call for evidence in relation to the potential creation of corporate liability for economic crime. This offence would be likely to cover instances of failure to prevent fraud, false accounting and money laundering, in addition to bribery and tax evasion which are already addressed in separate legislation. Five options have been outlined in this consultation including one, favoured by PwC, which uses a framework similar to the 'adequate procedures' defence set out in the UK Bribery Act.

Complicating the compliance landscape are differences in the prevailing regulatory regimes between the UK and other jurisdictions. Proliferating anti-bribery and corruption legislation, where the US Foreign and Corrupt Practices Act already permits facilitation payments that are explicitly outlawed in the UK, illustrates this divergence, and the uneven playing field it creates. Another difference is that whistle-blowers in the US are entitled to a percentage of the proceeds of a fine if their allegations are proved correct.

To help NEDs obtain a suitable vantage point on this threat and regulatory landscape, dashboard-style monitoring approaches utilising key risk indicators (KRIs) were discussed. These should track leading rather than lagging signals of emerging issues and potential compliance breaches. They should also verify control effectiveness across different factors such as political stability, terrorism, money laundering, corruption and cyber security using increasingly rich and insightful real-time data analytics.

A case study from industry was used to illustrate how risks that exist in overseas territories can often be very different to the risks that Head Office are focusing on. A 'bottom-up' exercise that effectively identifies and communicates risks in local territories can reveal significant differences to the 'top-down' approach from Corporate, so both should be performed and the results merged.

NEDs thinking separately about risk based on their broader experience and external perspective is also useful. By articulating a clear 'appetite' for the amount of risk that the organisation should be taking in its international operations and tracking evolving exposure on an on-going basis, Boards should be able to determine whether an unacceptable amount of risk is accumulating in individual areas of the global footprint. This mind-set should also insist that risk and compliance aspects are fully factored in to due diligence on potential mergers and acquisitions and that suitably robust controls are put in place as soon as possible in relation to acquired entities.

Risk and control levers for the global organisation

There are a number of levers that Boards can use to mitigate risks in overseas territories including:

Optimising culture

Culture needs to be broken down to specific behaviours that can be both more easily understood at the local level and more reliably measured. This needs to be reinforced by targets and remuneration that drive the right incentives and behaviours so that there is consistency between the values espoused by the companies and what employees actually see. Different cultures have different norms and exhibit different ways of working. Having a local national running an operation supported by an FD from Head Office can be a solution that works well to balance regional insight with corporate consistency. Alternatively, seconding local leaders to the Head Office for a period can have a similar alignment effect.

Other 'tools' that a NED can use to establish whether a local culture is good enough include:

- employee surveys
- analysis of incident reports/whistle-blowing mechanisms, including asking what is done with the outcomes of these processes
- feedback from key suppliers, customers and other business partners, including complaints received
- training programmes and continuous improvement programmes
- engaging internal audit or commissioning external audit firms locally to give a view on qualitative aspects.

'Tone from the top' in setting culture is often more established these days so the focus has moved to lower tiers of oversight, 'the message from the middle', and to equipping these cohorts to be true leaders in risk management and making them more accountable.

Simplifying the governance and compliance framework

Sometimes reporting matrices within organisations have become too complex, resulting in a lack of alignment between the legal and management structures. Companies should aim to:

- Adopt a simplified governance structure that drives consistency and clearly allocates accountability organisation-wide.
- Ensure there is a focused group-wide ethics and compliance programme to provide comfort at Board level.
- Have a robust Enterprise Risk Management approach that ensures risks are identified, managed and reported locally ('bottom up') as well as centrally ('top down').
- Strike the right balance between centralised oversight and examination, leverage of local knowledge of risk and business customs and encouragement of entrepreneurship and innovation.
- Encourage a group wide focus on transparency.

There needs to be sufficient focus and debate around this in the Boardroom. In some instances, Audit Committees with independent members at an overseas territory level can add real value.

The second line of defence is becoming increasingly important outside of FS in an advisory, facilitating and monitoring capacity but there is a need to ensure that the first line does not abrogate responsibility to the second. Internal audit, from an operational perspective, and external audit, from a financial perspective, can also help to provide appropriate checks and balances.

Internal audit

For global organisations with a significant footprint in high-risk locations and with a portfolio of potentially challenging third-party relationships, it is critical to ask some rigorous questions of the current state of their Internal Audit functions including:

- Is the audit plan sufficiently risk-based or does it still rely too heavily on criteria such as headcount or turnover in selecting where or what to audit?
- Is the audit plan flexible and able to shift according to changes in the internal or external business environment or is it too dependent on a fixed cycle?
- Is internal audit proactive enough to prioritise the heightened exposure when a new operation is starting up in an overseas territory or following M&A?

Internal audit is the third line of defence and is heavily relied on by Boards and Audit Committees. It is becoming more risk-based and is asked more often to opine on culture. However, a recent PwC survey found that:

- 44% of stakeholders report internal audit contributes significant value
- 18% report that their internal audit function plays a valuable role in helping their companies anticipate and respond to business disruption
- only 9% of respondents consider internal audit to be a trusted adviser.

This may be a function of rising expectations from 'end users' combining with the increasing scope of coverage for audit plans, encompassing ever more specialist areas such as cyber security or data protection. Selective co-sourcing of internal audit can be of value in larger organisations, as can outsourcing to a local third party, perhaps alongside the local statutory audit in complex or high-impact overseas territories.

Fully leveraging technology

As well as being a source and accelerator of risk in overseas territories, new technologies are increasingly directing global organisations' Governance, Risk and Compliance approach. Technology solutions exist that can be used for:

- horizon scanning and real-time monitoring, including the ability to track key risk indicators
- Cloud based solutions to control implementation and harmonisation challenges
- the provision of high quality and user-friendly management information around organisation-wide risk, compliance and control performance.

Companies should also consider using proliferating social media channels to supplement their due diligence on third party relationships as well as researching perceptions of their own business entities in overseas territories.

Strategic resilience

Given that it is difficult to make specific preparations for non-specific risks, the best long-term solution is to ensure the business has strategic resilience: that it has the attributes in place to withstand unforeseen shocks, and exploit opportunities, associated with currently unknowable major future changes to the operating environment anywhere in the world. This can be achieved through attention to resilience characteristics including:

- **Diversification:** of markets, products, customers and suppliers, ability to draw on variable sources of finance.
- **Recovery capability:** of manufacturing sites and IT systems, supply chain contingency.
- **Flexibility:** liquidity and leverage, variability of cost structure and contracts.
- **Defensibility:** of key client relationships, extent of insurance coverage for key assets, level of protection for intellectual property, robustness of cyber security defences.
- **Trustfulness:** quality and durability of relationships with key stakeholders (regulators, customers, lenders).
- **Innovation:** ability to constantly evolve and improve both products and business processes.
- **Scalability:** of manufacturing sites to alteration and expansion to seize opportunities, adaptability and agility of staff.
- **Responsiveness:** speed with which vulnerabilities and opportunities can be perceived and adapted to.

Where controls prove insufficient and an incident takes place, recent investigations have highlighted the importance of providing 'extreme cooperation' with the relevant authorities in order to minimise sanctions. Earlier in 2017 the US Department of Justice provided a transparent list of the aspects they will consider in mitigation in the context of such an investigation. This useful checklist of cornerstone aspects that a risk and compliance programme should incorporate includes:

- risk assessment
- policies and procedures
- autonomy and resources
- the role of senior and middle management
- continuous improvement, periodic testing and review
- confidential reporting and investigations
- training and communications
- analysis and remediation of existing misconduct
- mergers and acquisitions
- third party management.

Warning signs and questions for NEDs

There are often a number of warning signs that Boards can be alert to:

- A **business unit is unusually successful** with local management 'controlling the message'. Management performance reviews rely entirely on locally produced data. Risk registers are incomplete or do not change at all between reporting periods.
- **Too high a level of local autonomy** allows management to make decisions in isolation – with associated checks and balances weak or absent, and there is scope for local management to override group controls.
- **Heavy reliance on third line assurance** that isn't borne out by the quality/frequency of such reviews. This could include no recent assessment of risk management or control effectiveness.
- The balance of risk and control evaluations is **tipped heavily in favour of self-assessments.**
- Operational effectiveness of risk management and controls **requires high level of local management integrity**. The group places reliance on accuracy of associated MI.
- High degree of **scope for local management to interpret** group policies and procedures. Limited review of adherence by independent policy owners.
- **Dominant management style** may prevent appropriate challenge to leadership decision-making or the use of checks and balances that are present. **Management is resistant to outside review**.
- **Governance, risk and whistleblowing arrangements** are opaque and over-complex. Patches of **incomplete segregation of duties** between key areas allows for override of controls.
- Cost or staffing pressures may leave key **risk management, control functions and assurance activities resource constrained**.
- There has been a significant **change in accounting or reporting procedures** and criteria.

NEDs can ask the following questions about risk management and controls overseas:

- Do we know what our key risks and controls actually are across the full footprint of our business?
- Is there scope for greater commonality and standardisation across geographies?
- What is the scope for automation and cost reduction?
- How can we visualise our control environment?
- Does our control environment deliver predictable, stable outcomes regardless of location?
- What evidence do we rely on? Is this consistently applied across the board?
- Is assurance delivered in the right places and at the right time?
- Do our lines of defence operate effectively in relation to each other?
- Does everyone across the organisation know what our desired risk-taking approach is? How can we track this?
- How do we know our controls are effective in every location? How can we evidence that?
- Do all of our people really understand their roles and responsibilities around risks and control?
- Is our risk management framework truly effective at identifying and escalating significant risks across all of our territories?

Finally, a suggested checklist was provided for NED visits to overseas operations, as follows:

- In advance, request and read through recent internal audit reports on the operation. If there are none, ask when/how it will feature in the audit plan.
- Upon arrival, ask to see the operation's risk register for the previous two reporting periods.
- Look for evidence of awareness of the company's values: are these displayed prominently and featured in local promotional material? Are local employees aware of them and do they understand them?
- Deviate from the agenda prepared for you: ask to visit different sites, go to the canteen and speak to colleagues there, ask to be introduced to key customers or suppliers to get their viewpoint.
- Select a key control and ask to be shown it operating in action. An example could be the conflicts of interest or gifts and hospitality register.
- 'Google' the company's name once you are in-country. The results may be different from what a search in the headquarter country will reveal.

Above all NEDs should be prepared to be unpredictable and go 'off piste' when on overseas visits.

44%

of stakeholders report internal audit contributes significant value

18%

report internal audit play a valuable role in helping companies anticipate and respond to business disruption

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. In many ways this is an exciting time to be a business leader.

However, there is a dark side to these exciting times with a dramatic growth in cyber threat over the last few years due to the greater attack surface that increased technology provides. Today there are more potential adversaries with more power, more access, more motivation and more impact. Often there are devices that could provide a route into a company's systems that are not even considered, such as vending machines in offices. Other attacks can come through networks that individuals might connect to, e.g. breaching the WiFi in hotels. Managing information risk is critical as failures can lead to economic damage, 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 poviders)
- politics, ethics and regulation (including GDPR)
- insider threat (corrupt, well-meaning, unintentional)
- continued rise of technologies which are outside the reach of law enforcement.

Recent large scale attacks include:

- River City Media which allegedly left 1.37 billion records open and unsecured on the internet.
- WannaCry ransomeware which infected more than 230,000 computers in over 150 countries, exploiting a vulnerability in Windows 7.
- A variant of Mirai (a botnet) which attacked modems and routers through a maintenance interface impacting c900,000 Deutsche Telekom routers.

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

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

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

Implications for Boards and NEDs

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

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

The richer the data, the greater the threat plus social media amplifies the risks. People can also have very different views of the risk involved. With millennials the default position is to share. Part of the issue is that information resides in many places and the sheer volume of data is a real problem.

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

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

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

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

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

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

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

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

51%

of businesses holding electronic personal data on customers likely to suffer a breach

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

Priorities

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

Seize the advantage

- Set risk appetite.
- Check that digital trust is embedded in the strategy.
- Ensure compliance with privacy and regulation.
- Challenge the balance being struck between speed to market and ensuring confidence in the security of new products and services.

Their risk is your risk

- Understand the extent of an organisation's interconnectedness.

People matter

- Build and maintain a secure culture so that people behave appropriately in the 'moments that matter'.
- Identify key individuals who could have disproportionate impact on the organisation if they acted maliciously.

Fix the basics

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

It's not if but when

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

Undoubtedly, in many cases, the Board needs to be spending more time on this area. There should be someone with digital age knowledge in the Boardroom and data needs to become a currency around the Board table. This will become increasingly important once the General Data Protection Regulation (GDPR) is in force and individuals only have to cite distress, rather than proving financial loss, to claim compensation in cases of data loss/leakage.

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

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

The conversation covered:

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

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

68%

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

Conclusion

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

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

In terms of breach response, Boards should consider:

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

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

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

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

£3.2m

fines for UK data privacy issues in 2016, double the prior year

Cyber security – stage 2

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

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

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

PwC/third party experts

Richard Horne – richard.horne@pwc.com

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

This workshop began with 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. There is 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, including the recent Petya attack, and the Board's role in setting direction and assuring outcomes – refer to the cyber security stage 1 workshop on pages 18 to 20.

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

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

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

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

Framework of seven cyber security governance principles

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

At the heart of this framework sits:

Real understanding of exposure

This is a consistent issue and needs to be a Board conversation about both threat and vulnerability, including issues such as:

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

Around this core issue are:

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

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

£1.9bn

committed by Government to protect the UK from cyber attacks

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 helps Boards to make choices and set a vision/strategy for cyber risk.

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

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

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

and what is the purpose of protecting it:

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

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

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

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

For internal threats, the spectrum was:

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

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

Rogue employees can be difficult to identify so systems need to be constructed so that any one individual cannot do too much damage. It was noted that the 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?

£20,000

= average cost to large companies of cyber security breaches over the past year with some reaching many millions

- 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.

Only 26%

of breaches currently lead to information being shared externally other than to a cyber security provider

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?

Getting 'the basics' right can reduce the level of 'noise' so that it is easier to focus on the more complex areas. However, it needs to be a dynamic process as businesses, and therefore risks, change.

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 crisis

The final section of the session began with a look at a case study showing a typical financial services breach response. The incident involved 500 compromised machines, 35Tb of log data, 1,300 formats and 600 billion events requiring analysis. The attack was 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. On the positive side, the level of anomalous activity provides plenty of 'trip wires' for detection.

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

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

223 days

= typical time between cyber breach and impact

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 are:

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

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.

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

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

The concluding questions at the end of the cyber security stage 1 workshop were revisited as a good starting point for NEDs – refer to page 20.

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

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

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 expert

Paul Robertson –
paul.x.robertson@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. There is significant 24/7 external commentary in real time and society has greater expectations, both of which combine to make crisis management more challenging than in the past.

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. Often crisis management gets devolved too far down the organisation and it is important that there is senior management involvement, encouraged by the NEDs. Frequently the response is to want to dive in and fix the problem and the Board needs to take a more strategic view with the executive team 'doing the doing'.

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, e.g. ethical breaches, fraud – these tend to already be very serious by the time they come to light which makes the time to respond even shorter.
- Operational disruption, e.g. a bank with payment failures – 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.

These different types of crises have remained in roughly the same proportions over time. Classic rapid onset events are up due to greater numbers of natural/environmental incidents but are often handled better than previously. Hidden crises have increased mainly due to cyber breaches. Operational breaches have risen due to increased interconnectedness. Strategic disruption is also on the rise due to technological and other developments.

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. Similarly, an unusual number of incidents happening close together creates noise which may be a prelude to a crisis.

Importantly, different types of crises can combine and NEDs should consider whether risk registers are being reviewed in the right way. Often the review does not look beyond individual risks to consider combinations and culture is not talked about enough.

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 and NEDs should consider what could wipe out the business even if this is unlikely. Plausible risks should be explored. 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%.

A couple of tools that can be used to get a handle on possible crises developing include:

- Formalised and objectified 'near miss' reporting. A lot can be learnt from operational disruption and asking the 'what if' questions but there is a need to overcome the natural reluctance to report bad news for this to be successful.
- Senior incident management staff having weekly calls at short notice to ensure firstly that they can join a call at short notice but also to look at what has happened over the past 7 days/is likely to happen over the next 7 days, constantly building relationships to develop a better response.

In terms of 'playbooks' to respond to a crisis, these should focus more on the reaction to a crisis than the cause, as crises envisaged may not be the ones that actually happen. The response needs to be based on the organisation's values and practised.

66%

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

US$375bn

economic losses from cyber crime in 2014

Recent crisis management examples

Four different cases were discussed as follows:

IT operations failure

A recent operations failure appeared to stem from a power cable being unplugged possibly at an improper point in the cycle or with workarounds not properly implemented. There was a failure to recover appropriately and a lack of end-to-end capability, partly as a result of outsourcing of or reducing the numbers of data recovery specialists. Not communicating properly to the end customers resulted in a reputational issue.

Physical hazard response

A recent tower block fire led to a scale of response issue with a lack of leadership and poor post-event planning, again possibly as a result of having scaled back resources.

Terrorism

In recent months, this has resulted in a new issue of 'invacuation', i.e. denial of access to properties, rather than evacuation. Often companies only have systems capable of telling people how to get out. The new breed of terrorist incidents requires different response plans and organisations need to consider their duty of care as well as their capability and limitations.

Cyber

The recent Petya virus was nothing to do with ransomware and has brought organisations to their knees with some businesses being forced to operate temporarily via WhatsApp. This has been the closest incident to date to cyber warfare and resulted in different recovery priorities. Plans were outstripped by events.

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 3 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 3 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.

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, as these generally focus on operational disruption, frequently 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. NEDs need to be prepared to go beyond management's view of 'reasonableness' in terms of thinking about how bad it could be. The Board's viability exercise can also be used to consider what could break the company.

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 so that there is an appropriate contact who will help with the response.

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.

These are worth using as a test with organisations. A company should always start from its values and priorities should then be in line with these.

Often a plan is developed once and not changed over time whereas it should be periodically revisited in the light of changing circumstances. 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. Practising the response with deputies is also important in case the key individuals are not available when the crisis hits.

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.

Outsourced providers also need to be appropriately incorporated into the planning for a crisis response. It is important to discuss this in advance and ensure there are appropriate provisions in contracts to the extent possible.

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, and ensure their risk management functions are also, as their company's response to a crisis may be viewed with these in mind.

The psychology of decision making under pressure

There was a discussion around the psychological impacts of a crisis. Uncertainty and stress can cause different physiological, emotional and cognitive reactions. 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. This is particularly relevant in the first phase of a crisis which is often characterised by uncertainty and confusion.

US$194bn

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

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. Confirmation bias can also creep in with individuals looking to relate points to something they have seen before. 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?'.

Ways of overcoming these psychological pitfalls include:

Experience and exposure

- Skill acquisition through practice.
- 'Normalisation' – knowing what to expect allows you to rationalise it.
- 'Stress inoculation' – preparation lowers the strength of your reaction.

Establishing good team dynamics

- Establish a 'superordinate goal' – your values/principles of response (e.g. 'no customer will be left out of pocket').
- Exposure enhances familiarity and trust.
- A representative to act as 'devil's advocate' to reduce risk of group think and keep the decision making honest.

Coping with stress at an individual level

- Dissociation – 'stepping outside oneself', e.g. making a cup of tea and allowing the brain to rest while it focuses on a mundane task.
- Mindfulness – paying attention to your physiological response.
- Grounding – increases ability to take in information.

How well the emergency services respond in a crisis was discussed with their clear delineations of responsibilities under bronze, silver and gold chains of command and well-practised plans. The issue with corporates is that there is not the same unity of command.

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:

- Are we learning from current and recent events?
- Where is that learning being applied?
- 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?
- What delegation exists between the Board and the executive team?

Innovation for the earth – technology's role in solving sustainability challenges

There is mounting scientific consensus that the earth's systems are under unprecedented stress. However, this is also an era of unprecedented change. The 4th Industrial Revolution (4IR), as defined by the World Economic Forum, offers unparalleled opportunities to tackle environmental challenges.

Companies, governments, investors and research institutions all have a role to play in ensuring that the 4IR is a sustainable revolution. The workshop was an opportunity to explore this further.

PwC experts

Celine Herweijer – celine.herweijer@pwc.com

Leo Johnson – leo.f.johnson@pwc.com

Rob McCargow – rob.mccargow@pwc.com

Ben Combes – benjamin.combes@pwc.com

This workshop began with a look at the high level context.

Context

We live in interesting times. The earth's systems have never been under more stress/threat while at the same time the 4IR is the fastest technology revolution ever. Previous industrial revolutions have often stressed the planet but this time the 4IR could be harnessed to be part of the solution.

PwC's 'Innovation for the Earth' report, launched at Davos in January 2017, looked at ten key 4IR technologies and their application to five climate change levers.

Ten key 4IR technologies

Initially PwC focused on eight key digital technologies but then added advanced materials and synthetic biology so the ten 'Technologies for the Earth' are now:

- advanced materials
- Cloud technology, including big data
- autonomous vehicles, including drones
- synthetic biology
- virtual and augmented reality
- artificial intelligence
- robots
- blockchain
- 3D printing
- Internet of Things.

It is often the combination of these ten technologies that is the key to providing solutions.

The 4IR technologies are already available and have moved from being in vitro to in vivo. The technologies also obey Moores law in that technological progress can continue to be exponential. For example, classic computing based on the binary 0,1 system will eventually be replaced by quantum computing that will be able to solve enormous problems that are not possible under classic computing. Quantum computing will lead to super intelligent AI and unimaginable processing speeds, e.g. something that would have taken from the start of time until now under classic computing will take only a matter of seconds with quantum computing.

Mapping to climate solution levers

In the 'Innovation for the Earth' report the top ten technologies were mapped to the five climate solution levers of:

- clean power
- smart transport systems
- sustainable production and consumption
- sustainable land-use
- smart cities and homes.

Taking as an illustration smart transport solutions, technologies can be applied as follows:

Autonomous vehicles

- Mobility on-demand services.
- Open-sourced driver assistance programmes.
- App-based autonomous vehicle networks.
- Autonomous vehicles in industry.
- Drones for real-time traffic data.

Virtual and augmented reality

- Virtual meetings.
- Virtual shopping.

3D printing

- Printed cars.
- Localised production reducing transport.

Advanced materials

- Advanced battery manufacturing.
- Graphene applications.
- Advanced carbon fibre composites.
- Nanotechnology in fuel cells.

Cloud and big data

- Vehicle-infrastructure communication.

Internet of Things

- Smart urban mobility systems, including transport and parking.

Synthetic biology

- Synthetic fuels.

Technologies can be applied in similar ways to other climate change solution levers and, as noted earlier, the real power comes when the different technologies are used in combination to reinforce and accelerate solutions. For example, the next generation distributed grid for power will combine advanced materials, Cloud and big data, blockchain, artificial intelligence and the Internet of Things.

Technologies will enable us to change industrial/agricultural/city approaches to build sustainable solutions. Examples of innovations that are coming to assist this include:

- Solar spray coatings for the glass windows of buildings to power the building or on car windows to extend the life of the battery.
- A hyper loop high speed train system which would reduce the journey time from San Francisco to Los Angeles, possibly with virtual reality to make travel more comfortable at 400 miles per hour.
- Electric planes.
- Real time use of drones to prevent illegal logging/fishing.

There has always been change and the world is good at adapting unless the change comes too fast. A number of the technologies that it was thought would take longer to develop are happening at a faster pace.

Companies and governments need to be alert to unintended consequences, e.g. social, economic, etc. The World Economic Forum (WEF) has previously struggled with engagement with big technology companies but has now opened a 4IR centre in San Francisco to 'allow us to much better understand the impact the tech sector has on society and the positive role we can play'.

41%

of air cargo 3D printable by 2035

Big technology companies are looking to partner with industry and WEF's new annual Impact Summit in New York in September will focus on technology and how it can be used to solve the Sustainable Development Goals. There is a growing realisation amongst international countries and governments that policy may not get there fast enough as many innovations are happening now. A T20 task force will therefore help to develop policy for the G20 to ensure a sustainable 4IR.

The starting point needs to be 'what are the problems we need to solve?' rather than 'what can technology do?' and safeguards relating to social consequences need to be mainstreamed which means that behaviours in this space will be important. There is currently no international system to govern this and there probably needs to be one so that the agenda is not dictated by the major technology companies. Other corporates need to get involved as well and this is starting to happen.

Disruptive technologies and scenarios for the future

An airport was considered as a case study for how emerging technologies could disrupt business models including:

- Car parking could be impacted by driverless cars returning to base.
- Internet shopping and drone deliveries may affect airport retail outlets.
- Virtual reality could affect air traffic revenues with people deciding not to travel.
- 41% of air cargo has been estimated to be 3D printable.

Even a relatively small decline in the various revenue streams could cause the airport to go bust and the same is true of other high volume/low margin/mass business models.

A model was considered with the x axis moving from a decentralised system on the left to a centralised one on the right and the y-axis representing non-innovative at the bottom to innovative at the top in order to explore different possible scenarios.

Rise of the machines

In the top right quadrant, there is acceleration of AI, machine learning and quantum computing leading to potentially 47% of white collar jobs being vulnerable to automation by 2035.

Singapore has contemplated automated transport leading to automated cities leading to a closing of its borders and universal incomes for its citizens.

This clearly has significant impacts for developing markets.

Global rationing

The bottom right quadrant is where technology works successfully causing vulnerability in the high volume, low margin, mass business model. As an example, 150% of bank revenues come from 5% of bank customers who are subsidising others. Single companies begin to be able to control sector after sector, e.g. Amazon's recent acquisition of Whole Foods. A death spiral of certain industries leads to unemployment and social unrest.

Survival of the fittest

In the bottom left quadrant, investment slowdown with reliance on pre-mass production technologies leads to the breakdown of formal institutions and political disruption. The traditional role of the State ceases to have legitimacy and autonomous zones develop.

Organised chaos/local hero

There is, however, an optimistic scenario in the top left quadrant. Decentralised, innovative technology solutions lead to inclusive economic growth and improving productivity. Local communities come together to govern and there are open borders for people and goods. This could become a reality if intellectual property is free and distributed.

Responsible technology

Society and business therefore needs to consider how to reap the benefits of technology while remaining 'safe'.

A recent estimate suggests that 30% of roles in the UK are susceptible to automation by 2030. There is therefore a need to consider how to upskill people appropriately and promote the responsible use of technology. AI needs to amplify natural intelligence to avoid social dissension.

PwC has developed a responsible technology approach and policy. In particular, four relevant issues have been identified for consideration:

Jobs and skills

- Widespread disruption to jobs as technology and automation substitutes for many existing roles.
- Technology impacts low and mid-paid workers most, although knowledge workers are also at risk.

Health and wellbeing

Physical injury and poor health from:

- excessive or improper use of technology
- poor working conditions associated with production of electronics.

Privacy, security and integrity

- Abusing personal privacy by collecting data about people and tracking movements without their knowledge.
- Security risks from hacking devices and systems through inter-connected networks.

Environment

- High energy, carbon, water and raw material impacts from production of electronics.
- High energy use of data centres and networks.
- Growth in electronic waste.

The responsible technology approach and policy aims to ensure technology works for business, people and the planet. The policy is underpinned by concrete initiatives already underway.

47%

of white collar jobs vulnerable to automation by 2035

Recommended actions

Finally, some recommended actions were outlined for NEDs to consider with the executive teams in their organisations:

- **Technology roadmaps** – Optimise technology roadmaps to realise sustainable technological applications.
- **Design principles** – Embed sustainability into design principles to ensure 'smart' development of 4IR technologies.
- **Earth challenges** – Take on, and invest in, earth challenges including the Sustainable Development Goals.
- **Collaboration** – Develop industry-wide collaboration to aid standard setting e.g. consensus protocols.
- **Responsible technology** – Develop a comprehensive technology policy for your firm, fully integrating and aligning sustainability into 4IR development and deployment.

Social media, digital tools and online hygiene for NEDs

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

The workshop was an opportunity to gain an understanding of some common digital platforms and tools and also consider online hygiene, with a specific focus on how NEDs can use these tools in their professional and personal lives. (The application of social media in business was covered in our May briefings – refer to pages 8 to 10).

PwC and third party experts:

Nick Masters – nick.masters@pwc.com

Sacha Wooldridge – sacha.n.wooldridge@pwc.com

Stephen Page, independent NED – sp@spmailbox.net

Context

Social media is a dominant force shaping society. Everybody has a digital footprint whether they want one or not. Two photos taken at the inauguration of the Pope in 2005 and 8 years later in 2013 illustrated how the smart phone had become all pervasive over that period. Facebook is now bigger than the entire internet was in 2008.

However, there are risks to the huge explosion in social media as PwC has experienced directly. 'Heelgate' where a PwC receptionist employed by a contractor was sent home for not wearing high heels broke while our online communication head was in a meeting with the firm's Supervisory Board. The story was shared 10,000 times in 24 hours. After 36 hours the story had been seen by 30m people. Similarly, the envelope mix-up at the Oscars went viral.

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

Common social media platforms

The most common social networking platforms at the moment are Twitter, LinkedIn and Facebook. Twitter is now widely used by business and for political engagement with journalists, as well as by individuals. Often people will have a separate personal and business Twitter account. LinkedIn, a business networking site, is extensively used by recruitment consultants. Facebook started as a platform for sharing with family and friends but is now also used by businesses.

Sitting between common social networking channels and image/video based platforms is Flipboard which aggregates content from social media, news feeds, photo sharing sites and other websites, presents it in magazine format, and allows users to 'flip' through the articles, images and videos being shared. Readers can also save stories into Flipboard magazines.

Common image/video based platforms are Pinterest, Instagram and Snapchat which have almost no text. Pinterest is often used to create mood boards where pictures are collected, e.g. to help with a design project. It is also being used by some businesses, including PwC, for infographics. Instagram is used extensively by individuals. Photos and very short videos (up to 20 seconds) are posted on personal profiles but it is often quite staged and more about broadcasting than engaging. Very short bits of text can be added and there is the ability to link to other profiles. Snapchat is an app for connecting with friends or following famous people. Photos and up to 10 second videos can be posted but disappear once viewed.

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

PwC is using these platforms as follows:

- Pinterest – to display infographics which can then be shared by others.
- Instagram – to share charity events such as Ride the Nation and One Firm One Day and show a more personal side to the firm.
- Snapchat – used on campus with a geofilter for recruiting and to distinguish the firm from its competitors.

Snapchat has advertising between stories which is often tailored based on an individual's internet browsing history. Instagram has no advertising yet, relying primarily on celebrity endorsements.

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

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

- Instagram is owned by Facebook
- YouTube is owned by Google
- Periscope is owned by Twitter.

These owners are therefore extremely powerful in the influence they can exert, enabled and underpinned by their vast repositories of personal data enriched by augmenting social profiles with search history, browsing history, purchasing patterns and email traffic on 'free' services (eg gmail). This information power allows platforms to provide 'relevant' advertising but also to shape the content that users see.

There are also some very significant international platforms including:

- VKontakte – Russian language with over 400m users
- WeChat – Chinese language with 1bn users, both social and commercial
- Tencent – Chinese language with 800m users
- Weibo – Chinese language with 250m users.

Today, the majority of social media platform use is on smart phones or tablets.

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

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

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

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

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

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

Individuals use social media for:

- News – sharing articles with followers to demonstrate an individual is up to date
- Marketing – including pre-approved materials
- Personal – more likely to engage if a message comes from someone you trust
- Specialism – demonstrating expertise.

Social media is popular because it is:

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

All of the above help with influencing or getting a message out.

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

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

Language is an important part of social media communications and needs to be appropriate to the platform – generally more casual and less formal. Emojis are used extensively, particularly in Twitter where there are only 140 characters (approx. 16 words) and emojis can help with tone. There are also many abbreviations in text speak. Hash tags are used in text with key words so that content will be visible to those searching by those words.

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

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

140 characters to a tweet

Digital communication and collaboration tools

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

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

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

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

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

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

Questions to consider

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

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

Online hygiene

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

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

This was explored further by focusing on eight key areas:

Social engineering and phishing

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

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

Social media

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

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

Individuals should therefore:

- Review the privacy policy and terms of service before signing up for an account.
- Set privacy options carefully and revisit them periodically.
- Never provide a work-associated email to social media.
- Not post age, date of birth, address or phone number.
- Decide what online footprint is appropriate and ensure your friends understand this too e.g. tagging in images, uploading your personal details from their address book.
- Be wary of connection/friend requests from strangers.
- Remember anything online might be seen by people not in the intended audience.

Passwords

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

Strong passwords can include:

- Length – longer = stronger.
- Complex or not?
- Base passwords on a phrase not a word.
- Passwords should be changed regularly.
- Do not re-use passwords on multiple sites.
- Consider using a password wallet.

There is conflicting guidance on changing passwords regularly and using a password wallet. Frequent changing of passwords sometimes causes individuals to email passwords to themselves leading to exposure from hacking and password wallets can also be hacked. Criminals seeking access to data will exploit the weakest link which may not be the password itself but the password reset mechanism. Risk aware individuals can mitigate this by giving false answers to set questions when setting up accounts.

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

Handling data

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

Individuals should:

- Only gain access to the data needed and delete it when finished.
- Use business-approved storage for handling work data.
- Ensure email recipients are correct (email address auto-complete can create problems).
- Avoid sending sensitive, unencrypted data outside organisations via email or by using public Cloud sites (e.g., Dropbox or Google).
- Understand what data is held and where it is stored (e.g. password protected.zip files, on the desktop).

Knowing what data you have and storing it safely in approved ways is a good place to start. Even better is not to hold the data in the first place – leave it in the office whenever possible.

Internet browsing

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

Individuals should:

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

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

Working remotely

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

Individuals should:

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

Physical security

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

Individuals should:

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

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

Encryption

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

- Strong encryption adds another layer of protection in addition to vigilance and physical security.
- Activate encryption on work and personal devices and only use apps which support secure storage.
- When possible, encrypt data in transit and at rest.
- Use strong passwords to ensure secure encrypted devices (e.g. complex PIN codes for mobile phone).

Setting risk appetite

There was much discussion of the need for every NED to make a well-informed set of choices based on the risks and the data they may hold now and in their future career. This risk appetite will shape the nature of their digital footprint and the level of protection that is necessary.

Individuals need to decide personally where they are on the spectrum from 'totally open and trusting' to 'private and paranoid' and then set their risk appetite accordingly. We discussed several profiles on this spectrum from a digital native who automatically and freely shares sensitive data to a highly risk-averse NED who operates several online personas choosing what to share and implementing strong protections for sensitive information.

It is possible that this risk appetite may vary for different areas, e.g. more risk averse with bank account data than other less sensitive information. Making the right decisions about social participation and information protection is becoming one of the critical choices for NEDs.

In 2008

the entire internet was smaller than Facebook's current size

Executive remuneration

Executive remuneration remains a matter of considerable focus for politicians, the media and the general public. There is a public perception of lack of fairness and real political impetus to respond to this.

The workshops were an opportunity to consider a number of the recent pronouncements regarding executive pay, as well as reviewing whether the 2017 AGM season had seen any real change in policy and practices.

PwC experts

Marcus Peaker –
marcus.peaker@pwc.com

Tom Gosling –
tom.gosling@pwc.com

Governance developments in executive remuneration

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

- The Executive Remuneration Working Group (ERWG) 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
- BEIS Green Paper
- Investment Association Guidelines (October 2016)
- ISS Guidelines (November 2016)
- Hermes Remuneration Principles (November 2016/February 2017)
- Norges Bank (April 2017)
- Legal and General (September 2017).

92%

of FTSE 100 LTIPs are performance share plans

The ERWG suggested Remuneration Committees should be trusted to consider alternative structures rather than being restricted to an LTIP model. They suggested the alternatives of:

- a standard LTIP with three years vesting and two year holding periods (which is the majority practice in the FTSE 100)
- deferred bonus (which can be tailored to the performance of the business each year)
- restricted stock (which is common in the US where it is viewed as an element of fixed pay).

However, despite lots of consultations, the recent AGM season has seen limited real change due to:

- the volume of the FTSE 350 needing to reset policy this year (c60%) meaning some investors have limited time to deal with the detailed and extensive consultation required to implement significant change
- insufficiently clear responses from investors when consulted
- the uncertain regulatory environment

There have therefore been very few changes to the standard LTIP structure and changes that have occurred have largely related to the introduction of holding periods for two years post vesting. A few companies went down the route of introducing different schemes but withdrew at the last minute because support was thought to be only around the 50–60% mark. This would still result in technical approval but some companies are hesitant to propose policies that are not guaranteed high levels of shareholder support. This raises the question of what is an acceptable level of support.

When remuneration practice is evolving, a lower level of support could potentially be viewed as acceptable. However, this did not sit well with the BEIS Select Committee's proposal that less than 75% support for a policy means that it needs to be brought back for consideration the following year. The Government's subsequent response to the Green Paper (see footnote) ultimately did not include a proposal to change the voting regime. However it did suggest that the Investment Association retain a register of companies that receive more than 20% votes against their remuneration resolutions.

There is also a concern about the level of power ISS have. Many companies consider the quality of their analysis to be good but there is a lack of engagement and often they do not commit to a point of view. There is a perception that ISS have also started to stray into areas of strategy and commercial judgement which could be considered to be the shareholders' role. The concern over agencies therefore needs to be addressed.

Further variations in level of engagement are seen amongst the institutional shareholders and investors need to meet companies half way and be prepared to give views. Blackrock and Hermes have indicated they are willing to embrace change and Norges Bank are not keen on LTIPs but have not voted against those companies that have retained them. Legal and General advocate a two year post retirement holding period.

PwC has been supporting simplification and restricted stock schemes but the UK market is complicating this with underpins to compensate for the increased certainty. More companies have therefore gone with deferred bonus in the few instances where there have been changes. Those companies that had done something different in the past and renewed this generally did not meet with resistance.

Most recent executive remuneration issues have been around the operation of the policy including:

- pay for performance
- focus on bonus outcomes (low tolerance to commercial sensitivity re target disclosures)
- exercise of discretion (only really permitted downwards)
- increased share ownership guidelines
- pension benefits.

Investors do not accept that executives can have too much interest tied up in a company even though the perverse unintended consequence exists of CEOs leaving to be able to access their shares. There is no real traction in a two year holding post cessation as CEOs do not feel they should be penalised for the actions of their successor.

In general over the past AGM season, most companies have maintained pay levels. Where there have been reductions to quantum, this has largely been the result of companies simplifying multiple incentives into one LTIP.

There has been a great deal of focus on fairness as the quantum will always look significant to the average employee. A Remuneration Committee can however explain how policies attempt to incorporate fairness and recommendations in this area are likely to come in to the UK Corporate Governance Code ('the Code') following the Government's invitation for the FRC to review this.

Pay ratios are also inevitable and BEIS support the CEO single figure versus median employee pay. The PwC view remains that pay ratios in isolation may be misleading and comparison across sectors. and even sometimes within sectors, will often be irrelevant. Ratios do not work well in industries where there is a great deal of flexible working or outsourcing. The only metric that may have relevance is the trend in the ratio over time and whether the gap is widening. However it is probable that, following the Government's response to the Green Paper, secondary legislation will be introduced by June 2018 requiring the publication of a CEO to average employee pay ratio.

There was a quick look at the pre-election party manifestos around pay and the Conservatives policies again raised the idea of employee representation on Boards, although Theresa May had seemed to be backing away from her previous strong stance on this. The FRC will review towards the end of 2017 how employee voice can be better presented to the Remuneration Committee.

Key emerging trends in executive pay for 2017

The majority of companies showed continued restraint in the operation of executive pay as follows:

- salary increases awarded in line with the wider employee population (around 2.5% in FTSE 100, 1.8% in FTSE 250)
- 33% of FTSE 100 CEOs had their salary frozen in 2016 (23% in FTSE 250)
- median CEO maximum bonus opportunity levels remained at 180% of salary in FTSE 100
- median actual bonus paid to FTSE 100 CEOs has gone down slightly from 137% to 120% of salary
- 92% of FTSE 100 LTIPs are performance share plans
- median CEO PSP award level has remained at 250% of salary
- median PSP term is now at least five years – either five years vesting period or three years vesting +two years holding.

The 2017 AGM season saw isolated incidents of voting against remuneration reports for the following reasons:

- level of payout
- targets not sufficiently challenging
- lack of target disclosure
- unwarranted use of discretion (upwards)
- increased/high incentive opportunity
- salary increase.

In terms of policy changes, the key policy changes that have been made were:

- simplification of packages
- increased shareholding requirements
- change in pension contributions
- added holding period on to LTIP
- increased quantum
- decreased quantum.

Overall, however, as noted earlier, there have been limited changes to policy to date. Any simplification tends to have been reducing the number of LTIPs rather than removing them completely. There were some companies that initially thought about changes but then chose not to proceed, others that discussed a policy change with their shareholders but did not get sufficient support and a few that published a proposed policy change but then pulled the AGM resolution as they did not think it would pass. This public withdrawal of proposals at the last minute is a new phenomenon.

2.5%

average CEO salary increase in FTSE 100 in line with employees

Looking forward

A White Paper was expected over the summer recommending a number of changes to the UK Corporate Governance Code in the following areas and coming into force in 2018. This White Paper was issued subsequent to the workshop – see footnote.

Executive pay

The current requirement is a binding vote every three years on remuneration policy and an advisory vote every year on the implementation of policy.

The BIS Select Committee proposal is that there should be a requirement for a binding vote the following year when a company receives more than 25% vote against the remuneration report. In addition, the Conservative manifesto wanted to legislate to make executive pay packets subject to strict annual votes by shareholders. (Neither of these are in the recent Government response).

The PwC view is that the current system works as:

- 10% of the FTSE 350 received <80% votes in favour in the last three years and one year later the average vote for the same companies was 88%, suggesting the majority had responded appropriately
- only 2% of companies are prone to consistently low levels of support.

There is also a sense that shareholders do not want a binding vote which is seen as more of a 'nuclear' option. They can in any case vote off directors annually if they wish.

Possible alternative executive remuneration structures that may be mentioned in the revised Code are:

- the standard LTIP model
- deferral of bonus into shares
- restricted share awards.

The predominance of the LTIP model will not change overnight but over time we may get to a range of practices that is closer to 50% LTIP/30% deferred bonus/20% restricted stock.

Pay ratios

This is likely to be the ratio of the CEO single figure pay to the average of all employee pay. A few companies have disclosed ratios early and demonstrate the differences between sectors. Some have also disclosed alternative ratios using mean rather than median.

Employee representation on Boards

This is likely to be in the Code on a comply or explain basis re how companies have engaged with their workers in this area. The idea of stakeholder committees seems to have gone away but questions still need to be addressed such as:

- which companies are covered
- how representatives are elected and who is eligible
- to what extent unions are involved in the nomination of candidates
- what is the proportion of worker representatives on Boards.

Various different models already exist in some European countries such as Germany, the Netherlands and Sweden.

Fair pay disclosures

An increase in the level of transparency in disclosing pay conditions for the wider employee population is also likely to be required as a step towards building trust with the public. Companies are beginning to talk more broadly about:

- pay ratios
- cascading of incentives to the wider employee population
- employee consultation
- gender equality disclosures.

There is definitely room for improvement in this area but companies should avoid boiler plate disclosures. Fairness does not mean equality but Remuneration Committees, and also the wider Board, should probably spend more time thinking about what it does mean in their circumstances. Unilever have already disclosed their 'framework for fair compensation'.

In response to a final question about whether the general move in executive pay is downwards, it was felt that it may be more likely to flatline. However, new executives are sometimes being brought in at lower amounts and therefore pay may erode over time as restricted pay rises. Remuneration Committees may need to consider whether talent will be driven elsewhere although there is greater normalisation globally than was previously the case.

5

years now median PSP term

Footnote:
On 29 August 2017, the Government published its response to the Green Paper consultation and recommended a number of changes to the UK Corporate Governance Code or secondary legislation.

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 treasury and the future of assurance.

PwC experts:

Dave Walters – dave.walters@pwc.com

Iain Selfridge – iain.selfridge@pwc.com

Jessica Taurae – jessica.taurae@pwc.com

Peter Hogarth – peter.hogarth@pwc.com

Alice Mason – alice.w.mason@pwc.com

Chris Raftopoulos – christopher.raftopoulos@pwc.com

John Patterson – john.t.patterson@pwc.com

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

Lynn Piercy – lynn.m.piercy@pwc.com

Peggy Gondo – peggy.gondo@pwc.com

Sophie Gates-Sumner – sophie.gates-sumner@pwc.com

Suzie Askew – suzie.askew@pwc.com

Accounting update

The first session began with an overview of IFRS 9 and 15 and the implications for Audit Committees.

IFRS 15 Revenue from Contracts with Customers

IFRS 15 is the culmination of a long running joint project between the IASB and the FASB to create a single revenue standard. It applies to all contracts with customers except those that are financial instruments, leases or insurance contracts.

It is effective for annual periods beginning on or after 1 January 2018 but entities that use IFRS are allowed to early-adopt the guidance.

The objective of the revenue project is to clarify the principles for recognising revenue and to develop a common revenue standard for IFRS and US GAAP that would remove inconsistencies and weaknesses in previous revenue requirements, provide a more robust framework for addressing revenue issues and simplify the preparation of financial statements by reducing the number of requirements to which an entity must refer.

There is a five step approach to achieve the core principle (of revenue recognised to depict the transfer of goods or services).

- Step 1 – identify the contract with the customer.
- Step 2 – identify the performance obligations in the contract.
- Step 3 – determine the transaction price.
- Step 4 – allocate the transaction price.
- Step 5 – recognise revenue when (or as) a performance obligation is satisfied.

Some of the areas have remained from IAS 18 but the key areas of judgement when applying IFRS 15 include:

Allocation of transaction price in multiple element arrangements – the guidance differs on allocation of transaction price which is now based on standalone selling price basis. A residual approach can only be applied in limited circumstances.

Accounting for contract costs – there is new guidance which was not featured in IAS 18.

Revisiting principal/agent – this area is now more focused on inventory risk and the indicator on credit risk has been removed.

Licenses – there is a whole new section on dealing with licenses.

New guidance on accounting for contract modifications.

Identifying performance obligations – there is now much more detailed guidance on performing this assessment.

Variable consideration.

For IFRS 15, attendees were left with the following key questions to ask management:

- Have key revenue streams been identified and compared to the new 5-step revenue recognition process for IFRS 15?
- What are the key policy choices, judgments and estimates that management has made upon transition and in developing new accounting policies? What is the process for review and approval of key decisions and consultation with the auditor?
- Does the company have the information needed to meet the required disclosure requirements of the new standards? What is the company's plan for enhancing disclosures through the period prior to adoption as expected by regulators?

IFRS 9 – Financial Instruments

IFRS 9 is also effective for annual periods beginning or after 1 January 2018. The objective of IFRS 9 is to address three specific components which were a response to a call for clearer guidance and earlier impairment:

- classification and measurement
- impairment
- hedge accounting.

This table presents the main changes between IAS 39 and IFRS 9:

IAS 39	*IFRS 9*
Rules based approach to classification	Principles based approach to classification
Bifurcation of embedded derivatives	No bifurcation for assets – one unit of account
Liabilities at FVPL – gains/losses in own credit in P&L	Liabilities at FVPL – gains/losses in own credit in OCI, w/out recycling
Incurred loss impairment model	**Expected** loss impairment model
Uncommercial hedging guidance	Risk management aligned hedging guidance

Some key questions to ask management include:

- How are management comfortable that the IFRS 9 classifications are appropriate (e.g. reviewing underlying contracts to ensure no problematic clauses)?
- How are management comfortable that the IFRS 9 impairment model appropriately captures the impact of forward looking information (including changes in strategy and the economic environment)?
- Have management evaluated where new accounting hedging might be applied under the broader beneficial guidance, and if so, how this will comply with IFRS 9 requirements?

Audit Committee considerations – what we would expect management to consider for these standards

Assess

- **Assess key revenue streams** against new IFRS 15 5-step approach and sample revenue contracts to validate or quantify conclusions.
- **Work closely with business units** to ensure full identification of all financial instruments, and underlying contracts.
- **Document approach** to adoption and establish governance and change management approach.
- **Identify areas of significant impact** and develop a project plan to address.

Convert

- **Analyse identified differences**, quantify impact on prior periods.
- **Document** accounting policy choices, key judgments and estimates.
- **Design processes** for applying new standard from date of adoption.
- **Identify disclosure requirements** and design processes for gathering information.
- **Draft financial statements** and disclosures for review and approval.

Embed

- **Educate and communicate** within the organisation.
- Implement **sustainable process** and **system changes.**

Finally, attendees were taken through the following areas Audit Committees should be thinking about:

- key judgments and estimates that could make a material difference
- whether the Audit Committee is educated on IFRS 9 and 15
- the impact on the Financial Statements
- process, controls and governance
- external communication, including disclosures
- considerations of allowable expedients
- is the company ready? If not, when will it be and what will be disclosed?

Treasury insights

The next session focused on treasury insights and what we are seeing at clients.

Supply chain financing is the concept of a supplier providing goods and services to a corporate, who then promises to pay the supplier, as per the terms of the supplier contract, via the supply chain finance (SCF) platform. The supplier then has the option to have approved invoices paid early but at a discount. This arrangement has tended to favour larger suppliers and has historically been a bank sponsored arrangement. Developments in fin-tech have seen these arrangements become more prevalent. As is the case for the larger bank sponsored programs, the accounting treatment for the trade payables involved in these arrangements will depend on actual facts and circumstances. These treatments vary between continuing to recognise a trade payable to recognising a bank borrowing. Audit Committees should also be aware that as of April 2017, all medium and large UK companies have a duty to report publicly on payment policies, practices and performance.

A further observed development is a growing market in securities backed by supply chain finance receivables. These arrangements often involve Special Purpose Vehicles (SPV), and some arrangements effectively amount to a corporate investing in their own trade payable. This raises numerous accounting questions, including whether the SPV should be consolidated and whether an investment should be recognised which are discussions Audit Committees should be involved in. Furthermore Audit Committees should ensure that treasury policies clearly set out whether this type of investment is permitted, as well as ensuring that an appropriate infrastructure is in place to invest in a diversified range of appropriate credit exposures.

Funding involving currency swaps and equity options

We have seen a number of examples where Treasurers, using a combination of complex instruments, are able to raise borrowings at reduced cost compared to more traditional and vanilla methods.

As an example, it has recently been possible to borrow Euros more cheaply by borrowing floating rate US Dollars and swapping those to fixed or floating rate Euros using a cross currency interest rate swap. Some points to consider would be:

- **Accounting impact:** numerous accounting questions can arise, including whether the interest rate floor that is commonly included in floating rate borrowing arrangements is an embedded derivative and whether hedge accounting can be applied.
- **Tax Treatment:** the impact on Group and Entity financial statements needs to be carefully considered as well as the tax treatment.
- **Governance and Policy:** the treasury policy on currency and interest rate risks should support this strategy if used.

Another example involves the use of convertible instruments and cash settled derivative equity options. The legal form and substance of these arrangements ranges greatly and opens up funds from a wider range of investors meaning the process can be considerably cheaper, and sometimes quicker, than the equivalent vanilla debt issuance or equity issuance. The use of equity options can help address equity price exposure or dilution concerns but does require careful analysis and explanation.

Complex accounting questions arise and often involve judgements as to whether these types of arrangements should be accounted for as a single debt instrument, one or more equity instruments, or other more complicated arrangements requiring the identification of embedded derivatives. The tax treatment also needs to be carefully evaluated.

The Audit or Finance Committees should be involved in discussions around setting up these structures and all structures will need to be re-visited once IFRS 9 comes in in January 2018.

Corporate Reporting/ Governance matters

The corporate reporting/governance update covered three agenda items:

The 'stakeholder agenda'

Following a number of high profile instances that have led to questions as to whether Boards consider the full range of stakeholders in their decision-making, there has been a significant government-led focus on corporate governance reform including a BEIS Select Committee Inquiry, followed by a Green Paper. The Green Paper, which was issued in October 2016, addressed three main areas: executive pay (voting, engagement with stakeholders, transparency and role of remuneration), giving stakeholders more of a voice and whether there should be a code or guidance for large privately held businesses. PwC published an initial response to these developments. *http://www.pwc.co.uk/human-resource-services/pdf/beis-select-committee-on-corp-governance.pdf*

In response to this renewed focus on governance, the Financial Reporting Council (FRC) has announced a fundamental review of the Code (after initially undertaking not to amend the Code again until 2019), with a consultation expected in November 2017. The changes in government and the commitments around Brexit are likely to mean that change will ultimately need to be implemented through the FRC – i.e. as Code or Guidance rather than legislation – but it is not going to be dropped.

The debate on governance reform is happening at the same time as a number of changes to reporting requirements this year which are also relevant to the 'stakeholder agenda'. The ***EU Non-Financial Reporting (NFR) Directive*** introduces a non-financial statement within the strategic report for periods beginning on or after 1 January 2017 and applies to public interest entities with over 500 employees. This new statement should address the following areas (as a minimum):

- environmental matters
- the company's employees
- social matters
- respect for human rights
- anti-corruption and anti-bribery matters.

Although most of these are already part of the strategic report, the Directive has a different focus – the impact of a company's business. Specifically, it requires information on a company's policies in the relevant areas, along with the outcomes of those policies, and any 'due diligence' done on them.

As well as the non-financial reporting regulations, there are a number of other recent reporting requirements aimed principally at stakeholders. These are website reporting rather than annual report requirements and companies should check which apply to them, as the criteria and timing differ. It is notable that they are not primarily driven by the ownership structure of the company but by its size and impact.

UK Tax Strategy: a statement is to be included on a publicly available website covering approach to risk management, tax planning, risk accepted and working with HMRC.

Modern Slavery Act: annual publication of a human trafficking statement in a prominent place on the company's website.

Prompt Payment Policy: half yearly reporting on a central digital location to include standard payment terms, average time taken to pay and proportion of invoices paid late.

Gender Pay Gap: annual disclosure on the company's website to include the mean and median pay gap, mean bonus pay gap and proportion of men and women in each quartile of pay.

In addition to these reporting requirements, we drew attention to the ***Task Force on Climate-related Financial Disclosures,*** which is a G20 initiative to address the risks that climate change poses to financial stability, chaired by Mark Carney. For more information on the disclosures that the Task Force is recommending companies to make in future (and the implications for Audit Committees), PwC has published an overview. *https://www.pwc.co.uk/sustainability-climate-change/assets/managing-climate-risks-in-the-retail-and-consumer-sector.pdf*

The 'productivity agenda'

Much of the debate on the stakeholder agenda has focused on section 172 of the Companies Act, which sets outs the responsibility of directors to consider other stakeholders. Section 172 also requires directors to consider the long-term consequences of their decisions – recognising that employees, pensioners and others often have a long-term stake in the companies they are connected with.

Our second agenda item therefore looked at the ***Investment Association's Productivity Action Plan***, which is focused on what directors and investors can do to improve the longer-term prospects for UK companies by tackling their relatively low productivity rates – British companies lag behind the international competition on this measure. The IA plan, first issued in March 2016, identifies a number of principles that would help investors to support companies in making decisions to tackle this issue, including ways in which asset managers and other market participants and intermediaries can make the investment chain more fit for purpose.

The principle most relevant for Audit Committees is the IA's call for better information to be given in annual reports to help investors make long-term investment decisions, and the session focused on the guidance issued by the IA in May 2017 to expand on this. The guidance encourages companies to report on a number of areas relevant to productivity (including, amongst others, capital management, ESG and human capital and culture) and sets out a number of specific metrics to consider disclosing.

From September 2017 onwards the IA will monitor how companies are responding to the new guidance through its in-house proxy adviser service, IVIS.

Audit Committee terms of reference

Lastly, attendees were given a brief overview on the updates to Audit Committee terms of reference. The Institute of Chartered Secretaries and Administrators (ICSA) has updated its model terms of reference in line with the 2016 FRC Guidance on Audit Committees. Although these terms are not mandatory, Audit Committees should be aware of them to update their own terms of reference. The main changes include:

- More emphasis on 'links and overlap between the responsibilities of Board committees' – Audit Committee member to be on Remuneration and Risk Committee.
- Audit Committee chair to sign the Audit Committee report in the annual report.
- Audit Committee to consider whether a third party review of internal audit processes is appropriate.

Future of assurance

The final session focused on the future of assurance: specifically the role of technology, how this will impact people and skills, and the scope of tomorrow's reporting.

At PwC, as in other organisations, we have experienced the pace of change in technology. Currently, technology aids and supports us in performing the audit but, with the introduction of the next phase of technology such as robotics and artificial intelligence, we are expecting a greater impact. The session discussed questions such as:

- At what point will this scale tip and technology be performing the audit, rather than supporting it?
- What types of technology are already being used or being explored and how might they look and feel in the audit of tomorrow?
- What technology innovation are we experiencing at clients and how do these developments influence the manner and capabilities of an effective audit response?
- What is the role of human vs machine and how can they complement one another?

The session moved on to consider the potential disruption that implementation of these new technologies might cause. What impact would this have on people and the skills available in a company? Some of the discussion points included:

- What will the role of people be in a technology enabled audit and how will this impact the skill set available in your organisation?
- How might audit and finance function business models change as a result?
- What skills will we all be seeking? Technical skills will obviously be needed, but what do we mean by technical? How do we plan for the breadth from innovators and creators to operational support?
- How do we develop the finance professional of the future? This shift in roles and skillsets will lead to a greater role for people controlling the machines who are performing the audit.

There was an ensuing discussion on the potential changes to the recruitment model, should the role of people change in the audit. Currently, the PwC recruitment model sees the Firm hiring graduates who will go onto further their career at PwC or another firm as a CFO/CEO. With the changes in technology, we can see this 'pyramid' model changing to more of a cylindrical or even an inverted pyramid shape where we may not be supplying the FD/CEO roles needed in industry and could be recruiting in more qualified technology specialists. This then led to a discussion as to how the future CFO/CEOs will rise through the ranks if all organisations changed their recruitment models.

As the capabilities of the technology and the role of the people performing the audit changes, we discussed the potential impact on the scope of reporting, and the following questions were touched upon:

- If technology can enable assurance of more outputs more immediately, what could be the impact on the scope of an audit?
- Is there potential for a much broader set of information, beyond the annual report, to be considered?
- As technology changes how we deliver assurance, what will the parallel impact be on the digitisation of reporting itself?

Throughout the discussion it was clear that the exact timings of each of these potential changes is unknown but Audit Committees should be aware of direction and the pace of change. How auditors design and embed technology in delivering the audit will reflect how clients use technology and therefore there will be a mutual and related impact on all our organisations.

Contacts

Andy Kemp
Chairman, Non-Executive Director Programme

T: (0)7801 246976
E: andy.kemp@pwc.com

Liz Smith
Director, Non-Executive Director Programme

T: (0)7802 929150
E: liz.smith@pwc.com

170727-122754-LS-OS