Awareness, knowledge, communication and culture (Almost) to infinity and beyond

INTRODUCTION

This report encapsulates the views of more than 20 experts – from the worlds of risk management, digital risk, information and security, governance, business, insurance, law and HR – who took part in an Airmic roundtable breakfast on the important subject of governance for cyber risks. The discussion took place on 17 May at the offices of Paragon Insurance Brokers, London.

There is no slowing in the pace of change in the digital and networked world on which all our business models are now based. The consequences for boards are changing and escalating. . We must continuously revisit our cyber risk governance procedures, especially in the face of increasing regulatory and shareholder focus. This remains an important issue for Airmic members.

During our discussion, the lack of a common language was the most frequently-mentioned single issue standing in the way of good cyber risk governance. It holds the board back in building knowledge and oversight of the risks and opportunities of the digital world, and in sharing its strategic vision and risk appetite. Without that, the board cannot effectively shape the culture of the organisation in managing its engagement with the cyber risks that it wishes to take to build value, while also managing the exposures that arise from its operations.

We need a structure for that conversation to take place. As Airmic has always said, cyber risk is an enterprise wide, business-driven subject. It belongs within an enterprise risk management framework, with a line of communication to the board, probably through a risk committee or audit committee. Technology information and security expertise needs to be deployed to help the decision makers ask the right questions to build strategy and allow effective board oversight.

I am also concerned that there is a lack of education about the risks and opportunities of the digital world. We can do more to build education in these areas for our organisations, and for ourselves as professionals. We have to become digitally fit and comfortable with the subject. Just as people need financial literacy, the new literacy for the future is digital. If you're not fit for today, you're certainly not going to be fit for tomorrow.

From these observations, it is clear that there is a critical role for the risk manager in, developing a common language for cyber risks and cyber risk insurance, facilitating communication and increasing awareness and knowledge.

Julia Graham, Deputy CEO and Technical Director, Airmic

Action points:

- Drive the appropriate culture by placing the discussion in a business model and value-creation context.
- Build agreement on key language, even if it is only internally initially.
- Use technology, information and security expertise to help board members ask the right questions.
- Encourage more transparency and better communication from the board on its decisions.
- Make risk appetite an evolving process.
- Use scenarios and peer experiences to enhance board and senior management knowledge in the absence of good data.
- Facilitate greater board line of sight into and through the business.
- Place cyber risk clearly in the ERM framework and make it a standing agenda item for the risk and audit committee, and a regular report to the board.
- Ensure collaboration between experts (especially risk, technology, information and security) business functions at levels within the business and between businesses.
- Do not underestimate regulatory and other stakeholder interest.
- Understand the potential D&O exposures.
- Consider the expert support and value (beyond indemnity cover) offered by cyber risk insurance.
- Expect much more transformation and plan for potentially significant disruption.

The forces of change are accelerating and there is a palpable sense of urgency around cyber security. Airmic members must gather a coalition of change within their businesses, create a common understanding and a vision, inspiring and empowering their teams to make the necessary changes to how business is conducted. We must demand collaboration and stewardship from each other.

John Ludlow. CEO, Airmic

These are the questions we put to the group:

1. How aware and knowledgeable is the board about the dangers and opportunities of cyber technology?
2. What structures do we need at board level to give the board the best possible chance of exploiting these opportunities and addressing the challenges?
3. How do we secure and maintain board engagement?
4. How do we get good-quality management information on cyber to the boardroom, so the board can take high-quality decisions in this area?
5. How can we position cyber less as an IT risk but as a business opportunity, which can create wealth and value, but also see the business model damaged if the exposures are not managed?
6. How do we drive the right culture - the tone from the top, the mood in the middle, and the buzz at the bottom?
7. What are some of the technical issues we need to look at, including insurance and legal perspectives?
8. How do boards reassure stakeholders that they are on top of the issue?

AWARENESS, KNOWLEDGE, COMMUNICATION AND CULTURE (ALMOST) TO INFINITY AND BEYOND

Awareness, knowledge, communication and culture are essential to creating effective cyber risk governance. These are the conclusions of the group of risk managers, governance consultants, IT specialists and other experts brought together by Airmic in a roundtable discussion on cyber risk governance.

Boards are now aware of 'cyber' but do not feel confident of their knowledge, so they defer to experts, internal or external. There isn't a common language for discussion of cyber risk and opportunity. There is little history and the subject is not described in the framework that is familiar to boards for other risks, such as property or investment risks.

As a result:

- Boards find it difficult to ask the right questions of their experts.
- This diminishes their ability to identify the business implications of cyber risks and opportunities, provide effective oversight and, when necessary, take decisions.
- As cyber risk is unfamiliar to some, it can be difficult to create the right culture, the right strategic discussion and the right risk management response.
- Boards are anxious about being asked questions about cyber risk, by journalists and stakeholders which they cannot answer confidently.
- Personal exposures for directors are becoming serious. They need to be able to demonstrate board effectiveness in managing the issue.

Boards and senior management today are aware of the importance of cyber, but they are not necessarily confident of their knowledge. The key is to put cyber within the context of business value and build a common language. In that way, the organisation can understand its exposures from cyber and take advantage of its many opportunities. Continuing business transformation is making this essential. Board members need a level of knowledge and understanding that enables them to ask the right questions, as they would on other technical issues, but placed within a business conversation.

A major obstacle is the lack of a common language for cyber, even among professionals in the digital world. For board members and C-level executives from other professions, this makes it more challenging. There needs to be a distinction between a technical conversation and a business value conversation. They don't want a technical conversation about firewalls, access management, controls and vulnerabilities.

The board has a responsibility to take a long-term strategic view to generate shareholder value. Cyber is not just a risk, a threat that needs to be controlled, but also an enormous opportunity. Data is, for many companies, their biggest asset. While data protection right now is at the centre of the conversation, it's important to link data with the value drivers which make it the basis of business opportunity. Accordingly, the chairman has a responsibility to avoid giving all the responsibility for cyber to the director on the board who is an IT expert, but instead ensure that, collectively, directors can develop the necessary knowledge and expertise for a whole team discussion on the subject.

AWARENESS AND KNOWLEDGE

Board effectiveness and leadership are crucial. Boards deal comfortably with investment risk, financial risk and physical security issues, but they have frameworks and data going back many years. They are aware that cyber

is an important issue, but cyber is a young industry and there is little accurate data to help the board understand the risks. The result is a tendency to defer to experts but, without a common language, it is difficult for the board to use the experts effectively. If board members cannot ask the right questions, it diminishes their ability to work collectively to provide oversight and direction and create the right culture. They can also end up over-reacting to alarmist headlines.

"IF I TOLD THE BOARD WE HAD A DISTRIBUTION CENTRE WITH NO DOORS OR SPRINKLER SYSTEM, THEY'D GO NUTS. BUT THEY DON'T HAVE THE KNOWLEDGE TO HAVE THE SAME CONVERSATION ABOUT CYBER."

(AN AIRMIC MEMBER)

The essential driver underpinning considerations of cyber risk governance should be business value. Today, many boards and senior management have limited experience of technology but thousands of staff who have grown up with it. Their experiences are different. Against this background, trying to communicate the board's strategy on cyber risk appetite without a shared language is especially difficult. The binding factor should be the business objective. If this is clear enough, then everyone can understand how what they do is relevant to the risk and the opportunity, cyber or otherwise, regardless of age and experience.

The approach needs to be methodical and structured, starting with a risk assessment and an understanding of the types of risk that the particular organisation faces. Getting the board to think about the implications on customers or clients of a major downtime or a loss of data can succeed in moving the subject onto the agenda.

The lack of good management information on cyber risk probability and severity is a constraint, but there are alternatives to the giant spreadsheet when it comes to managing cyber risks. One method is using scenarios to work through possible events and their consequences. Another is to listen to the experience of others in the same profession or industry sector who have suffered an attack and recovered from it. The potential losses tend to be fairly consistent from organisation to organisation. If someone translates this experience into the exposure for the particular business and puts it into numbers, this is something directors can relate to. The potential upside is that if an incident is well managed, it improves the organisation's reputation and creates opportunities.

"IT'S MAKING A DISTINCTION BETWEEN A TECHNICAL CONVERSATION AND A BUSINESS VALUE CONVERSATION."

RHYS JAMES (PARAGON)

As an enterprise-wide risk, to the extent that the board has an enterprise risk management committee or an equivalent, that's a good place for cyber to sit. Governing through a risk committee or an audit committee is generally a good approach. Cyber security should be a standing item for the committee, and it can be supplemented with the discussion on information security, so all the aspects of governance, people, process and technology can be combined into one update. Within the committee, you need sufficient technical knowledge, but most importantly, a willingness to ask the right people to contribute. The discussion should be open-minded, challenging and inclusive.

Providing expert knowledge to the board needs to be done in a language that makes sense to all directors. Non-executive directors with specialist knowledge and relevant business experience can have a role here bringing the two aspects together. Teaming less knowledgeable directors up with colleagues within the business who can work with them to them think through the possibilities and consequences is another way of building competence and capability. Some companies ask external providers to give briefings, which helps arm the board with good questions to ask their technical people.

"THE DISCUSSION OUGHT TO BE LESS TECHNICAL AND MORE SUBSTANCE."

JO IWASAKI (ACCA)

"DON'T START FROM THE TECH END AND WORK BACKWARDS. WE COME BACK TO THE LANGUAGE. START IN THE LANGUAGE YOU KNOW AND WORK THAT WAY. THE IT PEOPLE WILL NOT GET TO BUSINESS RISK. YOU HAVE TO START WITH THE BUSINESS RISK PERSON AND MOVE THEM TOWARDS IT."

JAMES TUPLIN (XL CATLIN)

The risk appetite should not be static. The successful businesses of the future will understand the continuous need to revisit and, as necessary, repurpose their appetite. The winners are likely to be those who are prepared to challenge their stated risk appetite and seize opportunities.

COMMUNICATION

Today, many boards and senior management have limited experience of technology but thousands of staff who have grown up with it. Their experiences are different. Against this background, trying to communicate the board's strategy on risk appetite without a common language is especially difficult. The binding factor is the business objective. If objectives are clear then everyone has the basis for understanding how what they do is relevant to the risk, cyber or otherwise, and regardless of knowledge or experience.

That will not happen unless the conversation takes place. The component parts need a working understanding of each other's roles and co-ordination. They shouldn't be meeting each other for the first time in the middle of a crisis.

The risk or audit committee and ERM are probably the best governance mechanisms through which to channel a flow of communication and information about cyber up and down the organisation. Cyber can be a part of the regular cadence of committee meetings, and here some discussion in detail is important so committee members can challenge it. The risk or audit committee can act as a common point of focus, conveying information to the board, enabling board members to ask pertinent questions, and distributing the message downwards as well. This draws stakeholders together and aligns them.

"THERE NEEDS TO BE ONGOING ENGAGEMENT WITH THE BOARD VIA A RISK COMMITTEE OR THE IT DIRECTOR, AND RECOGNITION THAT THIS IS NOT A PROBLEM YOU THROW MONEY AT AND IT WILL STOP. THIS IS AN EVOLVING THREAT. THAT'S IMPORTANT."

MIKE HAFFENDEN (CRF)

CULTURE: TURNING INTENT INTO BEHAVIOUR

"AS WITH EVERY OTHER RISK, YOU ARE TRYING TO PREVENT A BOX-TICKING EXERCISE AND TO BRING IT DOWN TO OPERATION LEVEL AND THE IMPACT ON CUSTOMERS, AND THEN BRING IT BACK TO THE BOARD ONCE THAT ANALYSIS HAS BEEN DONE."

(AN AIRMIC MEMBER)

Developing the right culture is everything. The tendency to treat cyber risk as a technical issue, and the lack of a common language, are barriers to establishing a good cyber risk culture. Cyber risks can appear so alarming that boards might feel overwhelmed, and inclined to become risk averse, but attempts to eliminate cyber risk will close down opportunities.

When it comes to corporate culture, there is often a gap between the board intent and strategic purpose, and what is being lived in the organisation. This is especially true with cyber where the experience of the board and its employees can be so different. It is important to understand the importance of, and drive, the right tone from the top, the mood in the middle, and the buzz at the bottom.

A board needs to be careful of the behaviours it is actually rewarding in the organisation rather than those it says are desirable.

It has to rely on the judgement and decision-making of a vast number of people in the organisation daily.

It should be creating the conditions for wise decision-making and judgement, and not be driven solely by regulatory and compliance considerations. Real-life work issues – contracts, incentives, the things that pay the mortgage – drive behaviours just as much as any broader talk about culture. As many examples have shown, a culture of report and remedy, not blame, is much more likely to produce good behaviour and self-reporting. There should also be a system of reward and recognition for early recognition of bad things.

"IF YOU HAVE A BLAME CULTURE, RATHER THAN REVIEW AND REMEDY, YOU WILL INEVITABLY BE FIGHTING FIRES FROM DAWN TO DUSK."

ROBBIE STAMP (BIOSS)

The board can take the lead by being more transparent about its discussions. Board members should also meet as many people as possible at different levels of the organisation so they understand people's daily experience of working with cyber. Employees can find themselves forced into a choice between getting their job done and complying with unnatural security procedures. The real trick of culture alignment and cyber awareness throughout the organisation is to make it easy for people to do their jobs in the right way.

A shift in the ground-level awareness of cyber away from fear and to business advantage is more likely to motivate people. They will see the opportunities to generate more business. It's a shift they will want to embrace.

What people – both directors and staff – pay attention to sends signals. What they don't pay attention to sends as many signals.

There are cultural differences between countries, regions and even functions. The culture of IT security is very different from that of the risk management department or HR, for example. In the past, the IT people were left alone to get on with things; today they are being asked to collaborate with people who have different ideas of risk.

The greater the board's understanding and effectiveness in cascading that messaging, the more effective the organisation will be in building not just the cyber risk culture, but an enterprise risk culture. There isn't a single method that will suit every organisation; it needs to be tailored and take advantage of what's already there. Again, agreeing a common language is an important starting point. Nor is it limited to cyber risks. It applies to how everyone is encouraged to behave in the organisation.

One route into cyber awareness is education that helps people be more secure in their private use of technology. People appreciate having better security for what they do at home and what their children do on the internet, on social media and so on. That can translate into better cyber behaviour at work, provided they understand why it's important, and the message is consistent from the top.

"PART OF THE CULTURE IS THAT EVERYONE IN THE ORGANISATION UNDERSTANDS THAT PART OF THEIR JOB IS TO MITIGATE RISK. EVERYONE IN THE ORGANISATION IS A RISK MANAGER."

DAN LICHTENSTEIN (GRANT THORNTON INTERNATIONAL)

Is this an area where the risk professional can facilitate?

NO SUCH THING AS 100% SECURITY

Cyber needs to be part of the ERM framework – it is a question of understanding the likely cost of failure to provide the product or service that's affected. One way of thinking about it is as a non-damage business interruption loss.

Anecdotes from business risk managers recount how a board will just want to know whether its cyber risk is managed, with a yes/no answer. They want it done and they want it bullet-pointed. The aim must be to start by giving directors better questions to ask the people at the business level.

When it comes to cyber risk insurance, there is still a need to build awareness and knowledge, and the market is evolving. Cyber presents three main bundles of risk:

- Balance sheet: cash to respond to an incident
- Business risk: the impact on clients and business partners, resilience in terms of returning to action, shareholder concerns, ability to hire and to raise capital in future
- Liability costs: clients, contract issues or regulators.

For practically all businesses, cyber insurance offers value under all three headings. For most companies, it provides the finance to support the crisis response,

IF YOU'RE NOT MANAGING THE INCIDENT PROPERLY, IT'S NOT JUST YOUR REPUTATION AT RISK, OR JUST WHAT YOU'RE SAYING UNPROMPTED TO THE PRESS WHEN YOU GET DOOR-STEPPED. IT'S ALSO HAVING THE REGULATOR SITTING THERE, WATCHING WHAT YOU'RE DOING - THE VERY FIRST QUESTIONS THEY ASK ARE AROUND GOVERNANCE AND LEADERSHIP. THEY ARE READY TO JUMP UP AND BITE YOU IF YOU'RE NOT DEALING WITH THE INCIDENT IN A PROPERLY STRUCTURED WAY.

Greig Anderon and Andrew Moir (HSF)

which will protect the balance sheet and limit damage to reputation. The quicker a company can respond and restore business, as well as dealing with the media wisely, then the better it can manage its reputation. Cyber risk insurance also provides expertise in a crisis, and recovery from incidents. Stakeholders are now little surprised when cyber risks materialise, so experience shows that a well-managed incident can enhance the reputation of a business.

"IF YOU ARE EXTRICATING YOURSELF FROM AN EVENT WELL, YOU ARE NOT THE ONE WHO IS HITTING THE HEADLINES AS THE ONE WHO HANDLED IT BADLY. EVENT MANAGEMENT IS DIRECTLY TIED TO REPUTATION."

LYNDSEY BAUER (PARAGON)

IT'S GETTING PERSONAL

Cyber risks are now a top agenda item for regulators. The board must be aware of the enhanced legal and regulatory risk that cyber is generating around the world, and that the framework is becoming increasingly complex. The regulator is going to the top, and their very first questions are around governance and leadership. Where organisations haven't performed well, regulators have introduced significant regulatory oversight programmes that have forced boards to move more quickly than they wanted. Regulators, also, have been recruiting highly skilled cyber security professionals, so they ask very pertinent technical questions.

Regulators will even attend scenario planning meetings, so they can see what might happen in an industry if there were a serious cyber breach involving a significant player. If there is a cyber incident, they may also sit with the board to see how it is handling the crisis in real time, rather than reviewing the incident six months later.

D&O underwriters want to know what the board is doing about cyber security. It is now accepted that data is a massive asset and one of the biggest drivers of the shareholder value. Therefore, the hat the board has a responsibility to protect its digital property. If directors fail to do so, then the situation is likely to get personal. The risk of litigation in cases involving a failure to protect data becomes significantly enhanced.

THE CHALLENGE FOR ME IS IN THE WAY CYBER SECURITY PROFESSIONALS TALK ABOUT CYBER SECURITY RISK. WE ALL TALK ABOUT IT IN DIFFERENT WAYS – RISKS, THREATS, CONTROLS, VULNERABILITIES... THE TERMS GET USED INTERCHANGEABLY. IF WE DON'T HAVE A COMMON LANGUAGE AS A PROFESSION, IT BECOMES INCREASINGLY DIFFICULT TO HAVE ROBUST AND INFORMED DISCUSSIONS WITH BOARDS AND BUSINESS LEADERS

MATTHEW MARTINDALE (KPMG

"IF I WERE ON A BOARD, I'D WANT SOMEBODY WITHIN THAT ENVIRONMENT WHO REALLY KNEW WHAT THEY WERE TALKING ABOUT, SO WE COULD HAVE THE BEST CHANCE TO PROTECT OUR OWN REPUTATIONS AND THAT OF THE COMPANIES"

HAROON MALIK (FUJITSU)

(ALMOST) TO INFINITY AND BEYOND

Anyone advancing in cyber space will be exploring opportunity, and with opportunity must come capability. Strategic planning is ultimately a responsibility of the board. It should have an item on its agenda at least once a year to look at the digital strategy and consider whether the company currently has the capabilities needed to manage the opportunities that it is seeking. Taken from this perspective, technology will eventually become part of the conversation. In any business case discussion on new markets, new opportunities and new

ideas, then technology will appear somewhere in the conversation.

Many industry sectors will change fundamentally in the next five to six years and a large part of that will be driven by technology. One of the keys to an effective board will be a diversity of perspectives, based on a range of skills, knowledge and experiences.

How does the board identify the opportunities and ensure that the risks that come with new ventures are managed within the risk appetite? Some of the best ideas may come from new recruits because they will have been thinking about it before starting a new job. People in the middle, who will be the future leaders, should be the ones thinking about how they can turn these ideas into money rather than avoiding risk. In their view, opportunity and risk are being dealt with elsewhere; they are just doing their job. But business will fail if they don't innovate, and that has to be in the IT space and governance as well.

"YOU CAN HAVE BIG INSTITUTIONS THAT WANT TO PROTECT THEIR REPUTATION AT ALL COSTS, WHILE SMALLER ONES MAY BE MORE WILLING TO CHALLENGE AS THEY HAVE LESS TO LOSE."

JAMES CROTTY (NED)

"WE ARE ABOUT TO STEP INTO TRANSFORMATION LIKE WE HAVE NEVER SEEN BEFORE. WHERE IS THE STRATEGY FOR DEALING WITH THAT?"

PAUL DOREY (CSO CONFIDENTIAL)

The massive upside to cyber gets lost in many discussions. The whole world is facing a transformational agenda. The speed of change has been nothing compared to what's coming.

Most companies are already in the cloud. AI and robotics are starting to knock at the door. These all have a cyber dimension. It is demanding enough for the IT professionals to keep up with developments. The board needs awareness and knowledge to challenge them. This prompts the question – how will board members have appropriate awareness and knowledge and to ask the right questions on a specialist subject that moves so quickly? Whether it's an advisory board member from another industry or a partner, it is something worth exploring. The board needs people with both the technical and business understanding.

Boards need to support rethink their business with a cyber-enabled strategy. Big established companies often want life to carry on largely as it is, and may have difficulty adapting to the new technology-based and digitally-focused world order. Data breaches tend to be at the forefront of people's minds, but real problems can occur when a company changes something fundamental to the functioning of the business. Many IT projects are only getting bigger and more difficult to implement. When an international hotel reservation chain tried to introduce a new system of internet booking, it was so complex, and involved so many people around the world, that it was deemed too expensive and difficult, and was abandoned.

"THERE IS SO MUCH FOCUS AT THE MOMENT ON GDPR, THE FINES AND THE EXTENT OF THOSE FINES THAT WE ARE IN DANGER OF FORGETTING THE FIRST-PARTY RISK AND THE FACT THAT CYBER COULD DO AS MUCH HARM TO YOUR OWN BUSINESS AS THAT OF YOUR CUSTOMERS, AND THAT WORRIES ME QUITE A LOT."

(AN AIRMIC MEMBER)

AI is a great opportunity and possibly a global systemic risk. Those discussions need to be happening not just at the board but at a wider business community and government level. At the same time, digital and technology is changing the power of everyone within an organisation. People can make a big impact regardless of their position within the organisation, but the organisational hierarchy isn't changing in tandem.

We need much more education on these subjects from schools to board level. The risk management profession can do more to facilitate and encourage education in these areas than we have otherwise done. The basics of risk and insurance are still important, but we are not topping up that knowledge with what the future might hold as well as we should be. It's a big wake-up call for the profession.

We have to get digitally fit and comfortable with the subject. Just as people need financial literacy, the new literacy for the future is digital.

Julia Graham, Deputy CEO and Technical Director, Airmic

ABOUT HERBERT SMITH FREEHILLS

As one of the world's leading law firms, Herbert Smith Freehills advises many of the biggest and most ambitious organisations across all major regions of the globe. Its insurance and reinsurance lawyers have an outstanding reputation in complex, high profile insurance and reinsurance disputes and for providing strategic legal advice and representation to corporate policyholders. Herbert Smith Freehills is Airmic's Preferred Service Provider on insurance law issues and has assisted Airmic in producing a number of its technical guides over the past few years.

herbertsmithfreehills.com

ABOUT KPMG

A UK limited liability partnership, which operates from 22 offices across the UK with over 14,000 partners and over 1,400 risk specialists who are supported by our wider global network. With our full lifecycle of services, which cover all aspects of cyber risk governance from the board room through to the back office. Our experts include accountants, technologists, economists, actuaries, data scientists, lawyers, mathematicians, ex-regulators, law enforcement personnel, forensic investigators and pure risk specialists making sure you are best placed to make the right decisions at the right time.

Subscribe at **kpmg.co.uk/signup**

ABOUT PARAGON INTERNATIONAL INSURANCE BROKERS LTD.

A specialist insurance broker for professionals and organisations in the UK and internationally, providing independent and intelligent insurance that goes beyond the expected.

With market leading capabilities and experience in the financial and professional lines sectors, Paragon partners with clients to deliver risk transfer solutions, claims advocacy and risk management services with a bespoke, personalised approach.

paragonbrokers.com

ABOUT XL CATLIN

A changing world needs new answers and we're here to help find them. As a leading insurer and reinsurer, XL Catlin helps clients to move their world forward by finding answers to their most complex risks. From our broad range of property, casualty, professional and specialty products to our future focus on innovation. Our position in the market has been gained from decades of working closely with industrial, commercial and professional firms, insurance companies and other enterprises globally.

xlcatlin.com

FACILITATOR:

Seamus Gillen, facilitator of the round table, is founder director of Value Alpha, a twelve-year old advisory firm focused on governance. A Chartered Secretary and company director, previously Policy Director at ICSA, and the author for the FRC of its Guidance on Board Effectiveness, Seamus conducts board evaluations, facilitates board away days and runs director training and development workshops - specialist areas are governance, strategy, risk, compliance and ethics. He writes and speaks regularly on governance issues.

www.valuealpha.com (T: 07739 088208)

RAPPORTEUR:

Lee Coppack