StrategicRISK

February 07

ROUNDTABLE 2007

DEVELOPING A RISK CULTURE

Sponsored by:

AON

HUGH JAMES

Aon Global Risk Consulting

Aon Global Risk Consulting offers a fully integrated range of solutions from risk identification and control, to assessment and risk financing. We are constantly innovating and improving our risk financing solutions in order to better serve our clients' needs, and deliver an outstanding global service.

With 1300 staff globally with extensive and wide-ranging experience, in over 60 locations in 30+ countries, we are one of the largest risk consulting organisations in the world.

For further information about how Aon can help you, please contact:

Andrew Tunnicliffe
Business Development Director
Aon Global Risk Consulting
8 Devonshire Square
London, EC2M 4PL

Tel: +44 (0)20 7086 1873

andrew.tunnicliffe@aon.co.uk

www.aon.com

FPA#3631

Developing a risk culture

An introduction to the StrategicRISK roundtable discussion by **Sue Copeman**

Financial institutions, perhaps more than any other business sector, today face the need to comply with a myriad of regulations which inevitably touch upon if not directly impact their risk management and corporate governance. While most of our roundtable participants agreed that regulations such as Basel II may produce valuable improvements in some cases, there was a general feeling that mere compliance is no guarantee of good risk management and in fact may go against the spirit of the regulations, which is to achieve best practice.

There was also some discussion as to the accountability – or lack of it – of the regulators, should initiatives like Basel II prove not to be beneficial, in view of the significant costs that institutions have devoted to meeting their requirements.

Some participants also highlighted the danger that corporate governance/risk management can stop at or near the top and may not filter through to the lower levels which may be more incentivised by associated financial or promotional benefits. It was suggested that good risk management may still not be a part of many people's job specifications, with their employers simply taking it as read. There is also a need to strip away the mystique, relating risk management to the day-to-day activities of employees and basically getting on their wave length.

At a senior level, is it better to take a risk knowingly or unknowingly? This provoked some discussion. Directors may be reluctant to articulate the risk appetite on which they base decisions for fear of criticism if loss from a major risk occurs. But identifying and documenting a risk demonstrates awareness and a calculated decision, even if that risk later occurs.

There was consensus that culture rather than regulation has the greatest part to play in embedding risk management and corporate governance through an organisation. And culture change is one of the most difficult things to implement.

Many of our participants believed that businesses are still failing to understand the risks and costs involved with IT, relying on controls rather than understanding their exposures.

The panel concluded by discussing the problem – ever present for financial institutions – of fraud. It was agreed that organised major fraud is becoming ever more sophisticated – an industry in itself – and financial institutions are hard pressed to catch up with the criminals.

Sue Copeman,
Editor, StrategicRisk

Roundtable participants

Cary Depel, chairman of the Institute of Risk Management and compliance and legal director of IFX Markets

Mike Brierley, business risk director, Barclaycard

Sheryl Lawrence, head of risk and compliance, group operations, Lloyds TSB

John Meredith, consultant, Hugh James

Michael Porteous, senior consultant, Aon

Joe Traynor, manager – firms risk team, risk department, finance, strategy & risk, Financial Services Authority

Lisa Vanson, risk manager, Groupama Insurances

Operational Risk

Much of the value is not in the initial thrust but in the pause for reflection

MIKE BRIERLEY

CARY DEPEL: Starting with the big picture, we have a number of important topics, among which is the impact of Basel II. Basel II obviously involves financial services institutions which have had to make an election rather recently on how they are going to deal with how they calculate the operational risk requirement. There are a variety of elections one can make, but the one which could potentially provide the most benefit and which requires the most amount of risk management is the advanced measurement technique. Does anyone around the table know that this is the approach that their firm is taking or will take and, if so, have you any thoughts on how you've got where you are and where you are going to go?

MICHAEL PORTEOUS: We have done a lot of work in the last year in reviewing frameworks for large financial institutions and we have just completed a project recently for a large European financial institution which has taken the advanced measurement approach. Aon has developed a collection of operational risk data through loss claims histories and this focuses on precise loss data. And we have been very successful in taking that data and modelling it back against the client's advanced measurement model and looking at the gaps they have, particularly the unique event types.

A lot of institutions have significant gaps in the way that they have calculated their loss and frequency scenarios. We are finding it very beneficial to help them design scenarios, methodology and processes to help that take place and so that they can better understand where those gaps are.

There is a lot of room for further development in the quantification and better understanding of what the actual losses and scenarios are, and how the event types compare in industry data as a whole. My fear is that the skew is becoming quite wide because the actual operational risk data that is currently being used is not precise enough. This may create potential risks for the whole industry. Debate is beginning around how we make the advanced measurement models more precise. .

CARY DEPEL: Is the FSA doing any data collection or has it had any thoughts about how it is going to supervise people that are taking the advanced measurement approach?

JOE TRAYNOR: It is still evolving. There is a lot of reliance on peer group work, comparing all the practices used in similar firms that we see. We have just rolled together the approach to Pillar 2 assessments with the main Arrow work to tie those together better, so that essentially these two assessments should be consistent and also things like the Arrow ratings on the senior management capability of the firm, corporate governance types of things, are now deliberately tied in with the overall ICG (individual capital guidance) that is given. That is the sort of main approach. In terms of implementation of practice, it is fairly early days.

CARY DEPEL: You mentioned something about some of the governance aspects. There are a range of requirements – senior management controls, obligations, that type of thing – under MIFID (the Markets in Financial Instruments Directive) and roughly similar ones under CRD (the Capital Requirements Directive). Do people round the table have thoughts on melding those together in their business?

SHERYL LAWRENCE: I don't think we have got a lot of choice, because they are covering the same territory.

CARY DEPEL: They are slightly different. You can choose apparently to use them separately.

SHERYL LAWRENCE: Why would you want to?

JOE TRAYNOR: It would also run counter to the spirit of what we are expecting from firms. The exercise is supposed to be good business practice as well, not doing it just to satisfy the rules.

MIKE BRIERLEY: The rules establish the minimum standard. Everyone should aim for higher, as you say, blending the two together and adopting whatever works for the individual organisation. I agree with you, Sheryl. Why would you seek to differentiate? You would seek to operate with a blend of the two together at an appropriate level.

SHERYL LAWRENCE: And if you require something additional because one thing requires that then you just add it on as an extra.

MIKE BRIERLEY: Going back to the Basel II question, I have had experience of two institutions going through Basel II preparation, the readiness process or whatever one wants to call it. One adopted a standardised methodology and the other adopted a more advanced methodology. And I think the one that adopted the standardised methodology as a starter took a view of then moving on to an advanced methodology, perhaps when things had settled down and the processes were better established with the regulator as well as in the industry in general. I believe that many of the benefits are to come, because inevitably there is a learning process going on for everyone involved. It is a fruitful one that is of huge benefit, but inevitably there is a goal to achieve, a certain status by a certain date, and that drives decision making and drives thought processes. Once that initial thrust is over, there will be a useful pause for reflection and more value will start to come through. This value will come through because databases will be improved; people will have peer experiences to draw on; best practice will come out. Much of the value is not in the initial thrust but actually in the pause for reflection and the riches that come after that. That will become clearer once we can see the wood for the trees.

MICHAEL PORTEOUS: Can I ask those in financial institutions, have you designed a process or strategy or so on, to actually be able to prove tangibly the benefits at a certain period of time that will result from Basel II? Surely it would be highly beneficial to have a process measuring the tangibility of benefits so that you can say, for example, 'yes this process works, it is beneficial for our organisation and has given value for our shareholders'. If it doesn't, then what is the recourse for the last seven years and the huge amount that has been invested?

SHERYL LAWRENCE: The question is, if we have implemented Basel II because the FSA have said so, haven't we missed a trick?

MICHAEL PORTEOUS: Absolutely. I suppose my question is, how we prove accountability, how we can be sure that, going forward, it is for the benefit of business.

Are we having regulatory impact for the sake of having regulatory impact and then later on will it be proved that the costs outweigh the benefits and the return to shareholders and stakeholders in the wider economy is not sufficient? How do we prove that we have learnt from this experience in order to be able to make improvements next time if and when it is required? The same thing has happened with the data protection (privacy) laws in some countries. After much spending, some governments have bowed to public pressure and are now reducing compliance levels. Who reimburses the companies for ill-fated decisions of regulators or governments?

SHERYL LAWRENCE: If you think of what is driving regulation, these same companies have been in denial about their responsibilities to their shareholders and other stakeholders for a long time. And therefore the regulations have been established. Was it proportionate? Was it appropriate? It is up to us as business managers to implement it in the appropriate way. It is about you not relinquishing your own responsibilities as a business manager to start thinking and to start recognising that you have accountability to your staff, to your shareholders in terms of return on their investment to implement it appropriately.

MICHAEL PORTEOUS: Sure, but the governing bodies are asking us to implement a process whereby we can eventually carry out an audit process and say to the boards, 'well, this investment and this decision that you have made to invest in this project or this piece of work had the associated risks and you have made a costed risk based decision on that, which is that it is beneficial to protecting the share price and the longevity of your organisation in delivering value, which is the ultimate aim of using risk management properly'. So what are we putting in place in respect of the powers that be, the regulators and the people who issue these instructions to the whole country and the whole industry to go ahead and do that? Are we collecting data to help them the next time to be able to make risk based decisions on the benefit of implementing these large pieces of work?

Who reimburses the companies for ill fated decisions of regulators or governments?

MICHAEL PORTEOUS

Regulation in the UK is comply or explain, isn't it? and we definitely adopt that approach

LISA VANSON

CARY DEPEL: I am willing to admit that many firms are not doing that, although I understand what you are saying.

SHERYL LAWRENCE: I would question then whether our management practices are fit for purpose. Who is going to invest any money without looking at benefits realisation? That gets right to the heart. I would have thought that most businesses have learnt that lesson at least a decade ago.

CARY DEPEL: Senior management systems and controls and implementing CRD in one form or another are not optional.

MIKE BRIERLEY: But you have to admit there are choices.

CARY DEPEL: There is a limited menu of choices.

MICHAEL PORTEOUS: Not only is there a limited menu, but when a regulator comes along and says, 'you haven't complied, we are now going to fine you', what then? Could we say that you don't have the justification to do that because we can prove that the cost benefit is not there? Is there not a responsibility for the people who are being paid through the industry to say 'you've got to do it because this is a positive cost benefit that can be justified?'

SHERYL LAWRENCE: Is that not the whole idea of the consultation process?

CARY DEPEL: I would say that it is probably better placed for the industry trade groups like the Futures and Options Association and the British Bankers Association to compile that information and make that case on behalf of their sector. It would be great to have but most businesses operate on need to have.

MICHAEL PORTEOUS: At the moment it is an evolutionary process. We are all looking at this and asking is it going to work and deliver tangible benefits? We do seem to be going down the right path, things do seem to be improving rather getting worse. Time will be the determining factor. Businesses do seem to have a better understanding of risk and the need to manage it responsibly. Surely now that we have come so far, is it not prudent to start thinking about other bodies that we can use to make the checks and balances for the benefit of the industry? Is there not a need to provide a mechanism to allow organisations to justify their investment in risk management from a cost benefit basis?

MIKE BRIERLEY: It is a very short conversation if you have an American parent. It is a matter of "you must do it" and that's it. "Spare me the 10 or 20 pages of analysis about how this is also cost beneficial and justified."

CARY DEPEL: Moving on to the subject of shareholder value, how do we influence the board and influence the communications that go to the board and go to the public to demonstrate that the kind of things we do provide shareholder value? How do we manage reputational risks? Has anyone any thoughts on that?

LISA VANSON: As the organisation I work in is a mutual, we have to answer to our French parent, which is our main shareholder, so that makes life easier for us compared to other organisations. We don't need glossy brochures and in fact we don't communicate to the public at all. As a mutual operation, we operate very differently to most businesses. Regulation in the UK is comply or explain, isn't it? – and we definitely adopt that approach. We don't have to comply; we are not a listed company, so we do explain.

MICHAEL PORTEOUS: Isn't shareholder value exactly what this is all about. and that comes back to tangibility of benefits? Surely the shareholders are going to have something to say in five years' time if they see no tangible ROI?

SHERYL LAWRENCE: I would put it the other way round. Do we include the premium that good governance attracts to our share price in our benefits case? Our shareholders generally are the institutional investors and they certainly know what good governance looks like. They ask very pertinent questions about our financial statements and our share prices are directly attached to this. I think there is a very clear link between the benefits case and shareholder value.

LISA VANSON: I believe that sometimes in very large organisations good governance does not permeate very far down those organisations. So you can tell the story to the analysts and it's reflected in your share price, but how far truly does good governance go down? I have seen in large organisations that it hasn't permeated down that far. Even in smaller companies, it reaches down to a certain level and the managers talk a very good story to their peer group, but it stays there.

SHERYL LAWRENCE: That comes back to the first question about the impacts that Basel II, and I imagine Insolvency II in insurance companies, are having. It is about getting the management around this and the approaches and the extent to which management awareness is a core part of it. If it is not part of it, you are starting your journey very late, because I think that is the largest part of it. Initially it seems esoteric and unnecessary or whatever. I think that actually getting people to understand the framework and recognise it is fairly easy, but this is the difficult part. Getting them started on that journey as soon as possible is useful. It is only good business management under another name. It is about taking risk – fear – out of their lives.

MIKE BRIERLEY: I agree, but I do have a heretical thought. Good risk management, which Basel II is trying to improve the general standard of, is clearly a good thing. And it is just good management. You don't do good risk management on Tuesday afternoon and good management for the rest of the week. It is about good risk management at any point of the day. What risk management ought to be is providing tools, frameworks and approaches to help managers manage within the risk policy that has been set by risk management. Again, getting the culture right, which I think is the point that has been made, is the most important thing. If you get the culture right, the fact that perhaps some of the tools and approaches are not all connected together, or not perfect, actually matters less.

The heretical thought I had was that actually possibly Basel II has got in the way slightly of that. Certainly, in the case of one institution that I've worked in, we started out with what was generally considered to be a poor approach to enterprise risk management. But we put in place very aggressive and broadly successful programmes, and we changed the culture and put in the right policies and gave them the tools and approaches. This was taking off quite nicely, going to the place where management was comfortable, other stakeholders including rating agencies, which have an increasingly sophisticated understanding and demand for good risk management, were comfortable. Then Basel II came along, and of course this contained much which is just best practice, end of story. But as opposed to management saying 'we need to manage risk management well because this can add value to our shareholders and stakeholders in general, because it is a good thing; it is just good management', suddenly it becomes a matter of 'the regulators want us to do it'. What gets lost is why we have to do it. Suddenly, it's purely seen as something which must be done because the regulators say so. So actually Basel II, which undoubtedly will raise standards overall to some extent, introduces an element of compulsion, of ticking the box, that was not there before.

SHERYL LAWRENCE: Then human nature kicks in.

MICHAEL PORTEOUS: I echo the fact that I think a lot of very good work has been done in Basel II and I think that we have been distracted, as you rightly said, from the real issue of how we get effective risk management embedded into organisations and how we make the topic of governance effective right from the top. In my opinion, that goes straight back to the necessity of having a well structured risk management culture and getting the board to understand how important it is that they place themselves at the centre of this and lead the risk management initiative.

Without a strategically designed risk culture that enhances corporate governance through efficient allocation of risk management roles, responsibilities and accountability, I don't believe that risk management will ever achieve optimal effectiveness

SHERYL LAWRENCE: It does help occasionally though to have the odd incident!

MIKE BRIERLEY: I agree, it's the culture question. It's getting that right and then everything will flow. And clearly sometimes it's useful to say, 'well, the regulator expects to see x y z', but that isn't the whole of it and I think it is getting the culture right. I am not sure that Basel II has necessarily helped in that regard although overall I am sure it has helped in specific instances, where perhaps a good course was already being set.

JOHN MEREDITH: Is anyone aware of any institutions that are taking steps to try to control the culture of the

Even though someone may be the best person for the job, if they don't pass the test they are not employed

JOHN MEREDITH

people who are being employed over time and to mould the workforce into a certain mindset? Before the meeting began, we were talking about a particular insurance company that uses critical thinking tests to ensure that they bring on board people that think in a certain philosophical or cultural way. Even though someone may be the best person for the job, if they don't pass the test they are not employed. It is part of the process of building a workforce that is in tune with what the organisation wants.

MICHAEL PORTEOUS: I am working on a project at the moment where we are looking at the corporate administrative services department of a large global bank. They had a recent operational impact which was significant enough to open the eyes of the board to the fact that there was probably a whole raft of operational risks that had not been looked at, and therefore they began to question whether their operational risk appetite level and calculations were accurate, because they hadn't looked at any of them. We have now developed a methodology to help restructure the operational risk management process within this area of the business, with the aim of more accurately evaluating potential impacts on the business. We have reached the stage of assisting the organisation to recruit senior level management based on job profiles that have been carefully designed around the management of key risks, risk management tasks and specific potential accountabilities. Through consultation, the organisation has understood that it needs to recruit individuals that have personalities or behavioural characteristics and skill sets that lend themselves to specific risk management requirements and that map back to the cultural structure they have identified that is required to enable the change process to continue and to enable the culture to be set for the long term. They have developed well-structured annual management objectives for various risk management roles and are now actively seeking the skill sets to go with that. Without careful structuring of the internal risk management culture using the right people to drive it, operational improvements will be difficult to achieve and the risk management process will not be optimised. We are in the process of talking to HR and trying to get the whole culture model approved and we have culture specialists coming in. It all has to be technically designed so that they can get the right people in the right roles to enable culture change can actually work.

MIKE BRIERLEY: You get the culture you deserve and you get the culture you measure as well. I have had some experience of trying to drive a change through an organisation that takes it from a place where risk management is seen as done by someone else, possibly the central team, as opposed to risk management being everybody's responsibility as in a 'this is the way we do business' strategy. You have to convince people that they already do it, they just don't think they do it, and that there are ways of doing it in a more systematic, measurable and evidenced fashion. Then you have to build into people's objectives specific risk management elements and a common vocabulary – otherwise you get a 'tower of Babel' effect. Once you have that vocabulary and have embedded it in an organisation, then you need to introduce measurements. What gets measured gets done may be a cliché, but it's true. And you also need to embed it at the key moments. We've already talked about recruitment, but it's also at promotion. Being good at your job is not the only criterion for getting promoted. Hopefully you have to be a good manager, and being a good manager also includes being risk aware and being a good risk manager. Having the message embedded at those key nexus points is really important, or you are unlikely to have very much culture change.

SHERYL LAWRENCE: Apart from the usual making sure that you get it into the board room, you certainly need all kinds of things to support a culture change. You need tools; you need all sorts of things and actually that is quite difficult when you are trying to reach thousands of people who are at different stages of educational capacity or levels and types of jobs. You want to have a consistency.

MIKE BRIERLEY: I think what you need are the systems and consistency. You are not going to do it in two weeks or probably even in two years. Try five years! So you must be persistent and consistent. I think, Sheryl, you said earlier that we have created some kind of mystique and part of that is the tower of Babel effect because of the terminology. You do need to have a relatively simple approach.

LISA VANSON: I think there should be specific risk management objectives included in people's job profiles. But some companies think that it should simply be inherent in their role profile that they should be managing risk.

CARY DEPEL: I think that people are pretty much coin operated. And at the end of the day, if they do not see a benefit either in promotion or in the way in which they earn their money, they are unlikely to do it. That is pretty crass, unfortunately. What I don't see is the joined up nature of risk management with performance evaluations and things like that. In my own organisation we are beginning to put in place more specific objectives year by year. We have a general set of job descriptions, but each year there will be specific things that people are asked to do and those are sometimes linked to bonuses and pay rises and things like that.

MICHAEL PORTEOUS: I think that is how it should be done. It is the only real way of getting it embedded. Once you make it tangible and measurable, then you can go through the process at any level of the organisation right down to the shop floor and say, 'these are your risks, your management responsibilities and this is how you will be evaluated on your management performance of them.' By doing that, you break down any potential mystique around what may be required and what is expected in a risk management role. Ideally the language needs to be simple and uncomplicated. You have got to take risk management objectives and break them down into things that people can really

You get the culture you deserve, and you get the culture you measure as well

MIKE BRIERLEY

understand and relate it to their own personal psychology. They need to see it from the view: 'this is my job; these are my objectives; am I comfortable with achieving these objectives?' They can ask: what are the risks associated with achieving these objectives? and assess whether they have the skills or qualifications to mange them effectively. They can say 'I'm comfortable with doing it; I can achieve that; that will trigger my bonus and my family will be happy. I want to stay in this company and I want to achieve'. So, if you can break it right down to those basic philosophical and psychological fundamentals then I think you have a real chance of succeeding. And I have taken that approach with the boards of some very large organisations, government, private and public, and it does make it a whole lot simpler. People need to see their risk management role, be it at the board level, as a line manager or whatever, in their own capacity, in their own psychological world.

LISA VANSON: And have they adopted it?

MICHAEL PORTEOUS: Yes, they go ahead and sign off on risks. They say, 'yes, I understand that. I do that anyway, so what you're saying to me is that all I'm doing is making it a more formal and documented process'.

JOE TRAYNOR: I think there is a very good example here of the point that was made about the disconnect of the culture at senior management level and what goes on on the ground. You get a very good game talked by senior management, and they genuinely believe it, but when you go and talk to someone at a branch somewhere, what they care about is what is going to make them money. So it's not properly embedded in the remuneration structure.

CARY DEPEL: On the subject of risk information, we've talked about communication going up to the board but we haven't talked so much about it coming down from the board, nor about some of the things which companies lack, such as knowing their firms' appetite for risk. Where is it willing or not willing to take its risks? What is it most concerned about, and what is it less concerned about? What is it prepared to spend money on and what is it not prepared to spend money on?

JOE TRAYNOR: While the culture of some senior managements may have come some way in terms of embedding good risk management, it can still be difficult to try and get a coherent statement of what their risk appetite is. You mostly end up trying to infer it from revealed preferences, that sort of thing. Traditionally, senior managers have tended to be happier to do all their management by intuition, but now of course they have got to engage with the risk information.

I think that there's a concern too that, if they are taking these large risk appetite decisions and things then go wrong on the ground, they are going to get nailed for that, rather than being in a situation of organised chaos, where basically the thing that goes wrong can be connected with decision making lower down. It makes them more responsible for risk decisions that are taken, and that makes them reluctant to set out their risk appetite.

CARY DEPEL: In case they get it wrong or miss something?

JOE TRAYNOR: Absolutely.

SHERYL LAWRENCE: So there are psychological issues. But at the end of the day, I would have thought that a risk management system might be used more as a crutch though. Look, we took a risk, it's documented. OK it happened. That's what a risk is. But it was anticipated – it was not a surprise.

MIKE BRIERLEY: We took a conscious risk decision but things can go wrong.

JOE TRAYNOR: That is why organisations do not have a problem embedding a risk culture further down the organisation. A lot of people managing risk on the ground are quite happy with it because they feel that they've covered themselves by reporting the risk, but we don't see that same willingness higher up.

LISA VANSON: That can be because the senior people in some organisations can be quite risk averse. Others have more dynamism.

MICHAEL PORTEOUS: Doesn't this harp back to the problem with corporate governance and the fact that organisations are not getting real, effective corporate governance because of all the things that we've talked about, like the understanding of how senior management should really take ownership and manage and improve management of critical risks, and the psychological issues around having the confidence to do that? Once you've got those things in place then surely you get more effective and proactive corporate governance, rather than the lip service that I think is prevalent around the industry.

CARY DEPEL: How many corporate strategies, missions or strategic plans actually incorporate the idea that organisations are taking on a certain amount of risk with a certain amount of certainty?

SHERYL LAWRENCE: It is happening more.

That can be because the senior people in some organisations can be quite risk averse. Others have more dynamism

LISA VANSON

I know what happens in our organisation because we do most of our business electronically!

CARY DEPEL

MIKE BRIERLEY: I agree.

CARY DEPEL: Well, it ought to, because that's the way in which you can point to aggressive decision making based on evidence and get it wrong, and still not be hung out to dry.

MIKE BRIERLEY: I think it is increasing and I increasingly see segments of strategic plans which say, here are the various risk items, here is the impact of the strategic plan on that risk. It would be a pretty poor strategic plan that did not have that kind of analysis embedded in it. And I do see attempts in that direction.

SHERYL LAWRENCE: It is also becoming a lot more integrated in the way that it is disclosed. We are seeing the initiatives and the risk implications side by side so I think people are getting there. And that's an important point because otherwise, rather like controls, you can sometimes find risks without objectives – I call them 'orphan risks'.

MICHAEL PORTEOUS: I think the chief executives would like to understand how to better use risk appetite for decision making and investment purposes, but there is still a long way to go for senior people to understand what really constitutes and makes up risk appetite and how you use it.

LISA VANSON: I think they have been doing that anyway – it's just a new term that we use now.

MICHAEL PORTEOUS: It has been going on for quite a while, I'm sure. Effective CEOs have been looking at it.

LISA VANSON: It is the way that we use it now which is very different. It drives our capital.

SHERYL LAWRENCE: I'm not sure that I entirely take your point. I think that there's a bit more than that in terms of the fact we all have an inherent capacity for risk. You can see that just in the way we cross the road for instance. Those in the board room do not come to work and leave that tendency at home. There will be some who are gung ho and others who won't say boo to a goose. But in terms of actually articulating it – actually pinning it down and saying what things you are prepared to do and what things you are not prepared to do – they haven't done that before and that is very difficult. In fact, so much so that we think we need a framework. But actually you can just write it down because you have been doing it without realising it.

LISA VANSON: How do you write it down?

MIKE BRIERLEY: One thing that I did in a previous role around this whole risk appetite issue was to go through the many policies that existed and then basically cut and paste together all the expressions of risk appetite. Some were quantity based. Some were qualitative. I put them all into one place and said, "That's our risk appetite. Each of you has contributed to this in your policies. Now, let's discuss where there are gaps in it".

When we actually saw it on paper, they said, "My God, is that our risk appetite? I'm not sure it is collectively." Of course, that's not the answer to anything, but it was a very interesting exercise. You have to face up to it. Are we happy with that? Collectively no, and in some areas there were massive holes. Although the business was being managed, so there was an implicit expression of the appetite.

JOE TRAYNOR: When you do come to actually articulate the risk appetite properly, people are surprised at what is a realistic amount of risk that the organisation is running, perhaps because as individuals they are quite risk averse. When you look at the actual amount of risk that you have to live with, it can be quite large.

LISA VANSON: In your own organisation which is a regulator, there must be a difference between what you accept internally and what you express politically. You might be prepared to live with a considerable amount of risk, but you certainly wouldn't tell everyone. You've got to keep that to yourself. In other organisations, the problem may be staff fraud risk. They will tell the outside world that this is a low remote risk, while in reality, according to all the statistics, it is happening. It's just that we don't know about it. But you want to tell the right story, don't you?

JOHN MEREDITH: Does anyone see insurance as being a driver? Because obviously there are increasingly sophisticated insurance products becoming available, particularly in areas like reputational risk, and to gain that sort of cover there are a huge number of requirements on the organisation in terms of managing risk, for the policy to operate.

LISA VANSON: Insurance drives a lot of our work, for example health and safety. Most health and safety is driven by insurance risk – whether you are insurable or not. If you can get reputational risk insurance, I don't know what the requirements from an insurer would be.

JOHN MEREDITH: Some US insurers are now offering it. They go through a huge process to gather information about the organisation. It's the management of risk, and effectively what they are doing is moulding the two together. To obtain a level of cover, your organisation has to be at at least this level of risk management. If you like, it's mandatory risk management.

MICHAEL PORTEOUS: We have been doing a lot of work in that area, looking at remodelling insurance policy wordings based on risk-based information. We're looking to help insurers to develop new insurance products based on information that has been gathered and the improved sophistication of risk management information, particularly out of the financial area, Basel II for example, and cybercrime. There is a lot of scope to improve the types of policies. You might take different types of insurance, mix them together and then you've got a policy with a number of different clauses from different areas, so that you're getting a mixed policy rather than a standard one. I think this is going to produce a lot of benefits for insurers and clients.

CARY DEPEL: On the subject of IT-related risks, I'm sure that most of us have got a story to tell.

SHERYL LAWRENCE: A question rather than a story. Is it well understood? In fact, do we have IT risk, or do we have IT controls?

CARY DEPEL: What do you mean by that?

SHERYL LAWRENCE: I think that everything tends to be around putting lots of controls in and no-one really understands the risk.

MICHAEL PORTEOUS: I agree. I was involved in a large project in a major European insurance company involving global IT risk management. It was basically taking Basel II type concepts and looking at project risk and the way they managed their internal IT risk portfolio assets and risks. So we are talking now of actually looking at the cost benefits of projects and allocating potential

risk to large IT projects and looking at the business impact of that on the critical aspects of business lines. First of all, was being able to identify and quantify actual value of risk for, say, outsourcing a whole IT asset register within a whole business line, and then looking at the corporate aggregated risk and adding it to the operational risk value. I think a lot of organisations haven't taken that approach and potentially have an operational risk value that may be invalid because they haven't fully calculated the IT operational risk values in their overall risk calculations. If you go into an organisation and look at IT risk management frameworks as such in a detailed way and do those sort of business benefit calculations and have a project risk focus, then you start getting closer to the real value of IT risk to the organisation. Let's face it, if you turn off the main servers in many organisations, what happens?

CARY DEPEL: I know what happens in our organisation because we do most of our business electronically!

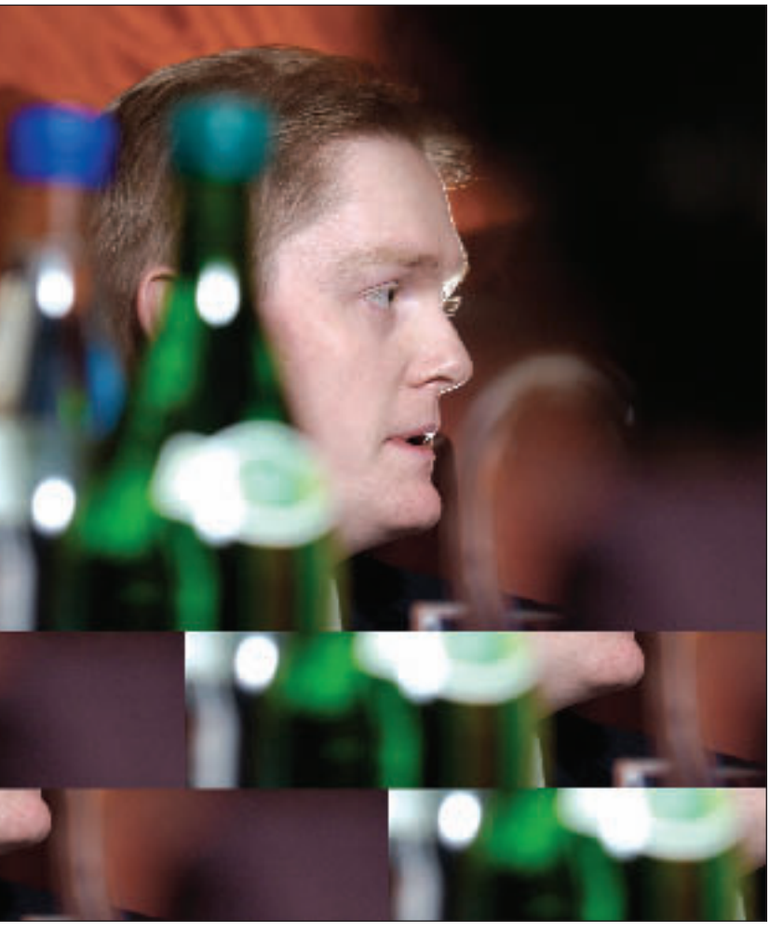
MICHAEL PORTEOUS: Exactly. And there is a big argument on what leads the business. Is it the business leading IT or is IT leading the business? Ten years ago it was probably the business that led IT, but is that true today? Maybe it's a combination of both, and it seems many organisations are underestimating the true value of their IT risk..

LISA VANSON: When you begin talking about downtime, you are largely moving into the area of disaster recovery.

MICHAEL PORTEOUS: That is one aspect and an important one, particularly when trying to calculate lost revenues, but what about risks associated to outsourcing, infrastructure or security for example? I think the exposures associated with this area are poorly understood.

I think that everything tends to be around putting lots of controls in and no-one really understands the risk

SHERYL LAWRENCE



I am not entirely sure that the money laundering drive actually took in all the principles of risk based regulation

JOE TRAYNOR

LISA VANSON: But that also applies to any element of the business that it's decided to outsource.

MICHAEL PORTEOUS: Absolutely, but IT is a critical function – the way that IT projects are managed. I think many IT project managers do not have adequate understanding of risk management. For example, if you're going to do a data centre merger between two countries, there are significant complex risk exposures to consider and plan for outside the technical IT requirements. Impacting risks in such a project may cause large disruptions to the organisation. Fine, you may have disaster recovery processes in place and back-up servers and so on. Recovering from an impact is one thing, but there are many other impacts and costs that are frequently unaccounted for. Critical exposures, that result from small risks may actually invalidate certain aspects of a policy for example. My argument is that, too frequently, organisations may be failing to calculate the full potential impact of IT-related risks on the value of the organisation and the associated share price.

CARY DEPEL: It is curious. In lots of other operational risks people talk about risk registers and that kind of thing. People do a lot of identifying risk exposures. When they can they do as much measurement as possible – frequencies, variety, correlation and aggregation. But what you have said really resonates with me in that people just go straight to the application and control procedures and actually very few people understand what the underlying exposure is.

MICHAEL PORTEOUS: Do you think, for example that a major credit card provider would be able to prove to the market the operational impact on the bottom line of a systems failure five minutes to midnight on New Year's Eve? I don't think they could do that, because you have got to go through the whole IT process and say what was the cause, then add up all the cost of downtime, and there would be massive reputational damage on top. Teams have to be employed to do the forensics and identification of what the problem was, the engineering of systems, there's a massive cost to an organisation. But someone show me where that value is represented in the operational risk register!

SHERYL LAWRENCE: I would have thought that many scenarios for Basel would have that sort of risk included.

MICHAEL PORTEOUS: Possibly in connection, say, with the scenario of what happens if a server goes down, how much is that going to cost us? Is the scenario with all these different components actually documented and causal chain impacts accurately calculated? Often the resulting values can be higher than originally thought.

CARY DEPEL: What are the weak links in the chain?

MICHAEL PORTEOUS: I think it is the failure to understand the value of the IT operational risk in the overall organisational operational risk calculation. And I believe it is also possibly the failure to understand IT itself. IT people understand IT and the head of IT risk and global security may understand the problems and the costs associated to managing the IT infrastructure well, but they always seem to be under-funded. The board understands operational risk as do the operational people and the chief risk officer. But chief risk officers frequently don't understand IT risk, and the IT people often don't understand the business requirement and objectives. Thus confusion arises and risks and exposures result. There is simply a knowledge and communication problem.

JOHN MEREDITH: Is it due to these language barriers? If they do talk, they use different languages.

MICHAEL PORTEOUS: Absolutely, language was a problem that came across when I did this particular project. There were completely different languages being used.

LISA VANSON: In some organisations IT expenditure is kept to a bare minimum, and therefore of course they experience downtime. The impact is a cost to the business. They will have reporting of the event – IT is often very strict on reporting. The only way to approach this is by quantifying the impact of all the downtime and then to talk to senior management and ask them what is their sensitivity on it. How much are you willing to invest? Their instinct is to reply 'nothing'. If you then ask that if you can prove that downtime over the year has cost a substantial amount, would they be prepared to invest, they will ask for the proof. If you can, then they will start looking at things like mirroring the systems on which the organisation is dependent. So if you can quantify the cost of the downtime, that gives you a very good story.

MICHAEL PORTEOUS: Downtime is a good start, it's one aspect, but then there are also the project delays, things like that.

MIKE BRIERLEY: Yes, downtime can be measurable, people can see that, but as you say it's all the other aspects – the inefficiency in the IT delivery mechanisms, projects being delayed or, worse, abandoned after two years and being started again. That's more opaque.

SHERYL LAWRENCE: That is where you get into difficulty if you apply Basel or Basel II because you wouldn't catch your income loss very easily.

MICHAEL PORTEOUS: How many IT projects in large global corporates get shelved every year?

LISA VANSON: You usually see a change of management as well.

MICHAEL PORTEOUS: Yes, a change of management

which isn't surprising. Well, what do you say to shareholders, "sorry about that, that was a huge waste and we're not going to be accountable for it"? I wouldn't stand for it.

LISA VANSON: And it is not just IT systems. It is projects generally.

MICHAEL PORTEOUS: It's the general programme and project management accountability. But I don't see it coming up on organisations' risk radars regularly as a critical concern. Some firms are waking up to it but it's not standard across the board. There's been a lot of focus on Basel II and managing main stream operational risk, but not so much focus on other drivers of businesses such as IT which actually runs the business.

LISA VANSON: You could say that that is part of their risk appetite though. They may have to go a certain way down the route of a project to see if it is going to be successful or not. If they have actually come to ground and they have perhaps got round a table and said "right, is this going in the way in which it was intended?" and the answer is no, then it may be more efficient to stop it.

MICHAEL PORTEOUS: How many organisations have a really well structured project approval process with end stage checkpoints throughout the delivery cycle that are validated and signed off by; audit, compliance, security?

LISA VANSON: It depends on how much money they are spending.

MICHAEL PORTEOUS: Exactly – cost benefit analysis. After you've spent more than the initial budget and you can see that you can only achieve 50% of the project's objectives, what is the no-go evaluation process, what's the business impact process, the cost benefit process?

LISA VANSON: Isn't this something that internal audit should check?

MICHAEL PORTEOUS: Sure they usually have some kind of remit for IT risk, but they don't really understand the intricacies of IT so the validation process is frequently ineffectively managed. There are very few IT specialists employed in internal audit.

MIKE BRIERLEY: And I think the point has already been made that an IT failure would cost maybe £10,000 to fix. But it might take someone a couple of days to figure it out. The impact on customers would cost maybe £50,000. Lost customers as a result could be 10%. The cost to acquire those customers again or replacement customers? Hold on a minute! £10,000 is not the issue. It is those extra costs that are a reliable way of convincing your management that this is a definitely a challenge. Not everyone is keen for those costs to be as transparent as that and it's a revelationary aspect of IT failure.

SHERYL LAWRENCE: That takes us back to the culture.

CARY DEPEL: And it also takes us on to our last subject which is fraud. It seems to me that there was a lot of effort when the FSA came into being, directed at things like anti money laundering, and we saw lots of big fines and other measures associated not just with money laundering, but also with not having robust systems and procedures in place. This seems to have settled down in the sense that people have got hold of those procedures and processes and by and large they are doing the right things and therefore money laundering is being taken out of the FSA sourcebook and being blended into senior management systems and controls. But the real emphasis now that I see coming out is on fraud, both internal and external. We certainly see that, where anything can be paid for by a debit or credit card, the amount of card fraud is absolutely going through the roof.

LISA VANSON: That is the reason for chip and PIN.

JOE TRAYNOR: I can absolutely confirm what you're saying. I am not entirely sure that the money laundering drive actually took in all the principles of risk based regulation. Much of the way it was driven was in a box ticking way rather than asking whether firms had got a system that's actually effective.

MIKE BRIERLEY: It wasn't risk based?

JOE TRAYNOR: Absolutely right. So the approach now is much as you said, Cary, taking the details out of the sourcebook and controls, and relying more on the steering group guidance. Interestingly, we are ourselves regulated. The Financial Action Task Force on Money Laundering, which is not risk based, has recently been asking us questions.like 'how do you check compliance in all firms every year with the anti money laundering rules?'

Now things have moved more to looking at things like fraud and getting these concerns onto the individual supervisors' radar, particularly on the fraud side. There is a feeling in some quaters, by and large that, although there is some disruption to the consumer, ultimately who pays for this? It is the firm concerned and there is a kind of logic in saying that if the firm can implement effective controls these would mean that it has a competitive advantage or is saving substantial sums of money. So presumably they would be doing that. As far as what the FSA should be doing, there is some controversy here as to how important fraud should be on our radar. From the centre there is certainly a push that the FSA should be concentrating more on fraud.

Not everyone is keen for those costs to be as transparent as that and it's a revelationary aspect of IT failure

MIKE BRIERLEY

There will always be people trying to exploit the gaps and commit financial crime – we're not going to have a crime-free society.

MICHAEL PORTEOUS

CARY DEPEL: You were saying earlier, Lisa, about how companies view internal fraud.

LISA VANSON: We have all got that as a risk. One of the fraud risks my own company has experienced arose in connection with a firm of intermediaries and we stopped dealing with them and reported it to the FSA to try to stop it happening to other insurers. But the FSA did nothing, so the people concerned moved on to other insurers. There is a history of insurers closing their accounts with these intermediaries without informing the FSA, but intermediaries are also regulated and, being a regulated company, they should have been closed. But the first insurer that experienced it merely closed the account and did not report it and others along the line suffered as a result. That is terrible. We should be able to share knowledge.

SHERYL LAWRENCE: Is there not an industry body to do that, other than the FSA?

LISA VANSON: Yes, but they've got no teeth. At the end of the day the FSA have got the teeth to withdraw a licence.

CARY DEPEL: This highlights the value of trade associations that are robust and work well.

JOHN MEREDITH: On the fraud side, there is a certain level of fraud, for example identity theft, where we accept that it goes on. It's been quoted that one in ten people are affected. In real terms the average loss is probably sustainable by the institutions in terms of individual amounts. Collectively, it is probably not. I have had direct experience of major fraud, and what interests me is the level of sophistication in perpetrating fraud and the fronting mechanisms and the time and the money that people will spend on creating a mechanism to produce what is effectively a perfectly legitimate company started by legitimate people who have been head-hunted from all sorts of places to give it credibility. This operation might take a year or longer to form and can cost £50m or £100m to set up because the nature of the fraud that will be perpetrated means that it will produce far in excess of this figure. I have come across a number of examples of that in the last six months. That to me is one of the interesting developments in fraud. In many cases it is organised crime. I am curious about that as a risk for the institutions and whether they can in any way really address it. That type of fraud is an industry in itself.

SHERYL LAWRENCE: It is big business.

MICHAEL PORTEOUS: As technology becomes more sophisticated in helping to deal with crime prevention, the investment required to commit cyber crime successfully will increase. While the frequency of impacts may reduce, in order for the fraudsters to justify the investment to commit the crime, they will seek larger returns for their efforts. Thus future single impacts may become larger and the methods or execution more complex. There will always be people trying to exploit the gaps and commit financial crime. We're not going to have a crime-free society.

JOHN MEREDITH: Looking at one particular claim that I came across, there were suspicious signs over a period of time that something might be going on, but nobody did anything about that information because they were concerned about reporting their suspicions. So what actually happened over a period of time is that they became, if you like, comfortable with what they were doing and did nothing about it. But when they look back, in hindsight those suspicions would have been a trigger for someone to actually investigate the firm. That brings up the issue, how do you get someone to have the courage of their convictions to come forward? In many cases, they don't have the right information. They're possibly concerned about discussing it because of their relatively junior position within the organisation. So they don't actually talk to somebody about their concerns.

LISA VANSON: That comes down to whistleblowing, doesn't it? Organisations need to give employees direct access to a hot line and make that known to people.

MICHAEL PORTEOUS: It also involves cultural aspects. As the fraud landscape becomes more sophisticated, we have to come up with innovative solutions to absorb the impacts. It may be that the impact is so great that a single insurer or a single organisation won't be able to absorb that impact alone.

SHERYL LAWRENCE: Should the insurers provide cover?

MICHAEL PORTEOUS: Well potentially they won't for certain types of risks. It might be a one in a million event but the impact may so significant that it may impact several providers at once. This may create instability in the market and force up premiums. That's part of the evolution and innovation of this industry. Maybe a solution is required to mitigate against large scale impacts? Such as creating a syndicate contingency fund to finance such events. What kind of a size of magnitude are we thinking about? Take global warming for example – have we started too late? We need to ask if we are growing cleverer and more sophisticated than the criminals. Sometimes I think we're not. Maybe the criminals are winning!

CARY DEPEL: It reminds me of that quote – soon we must choose between doing what is right and doing what is easy.

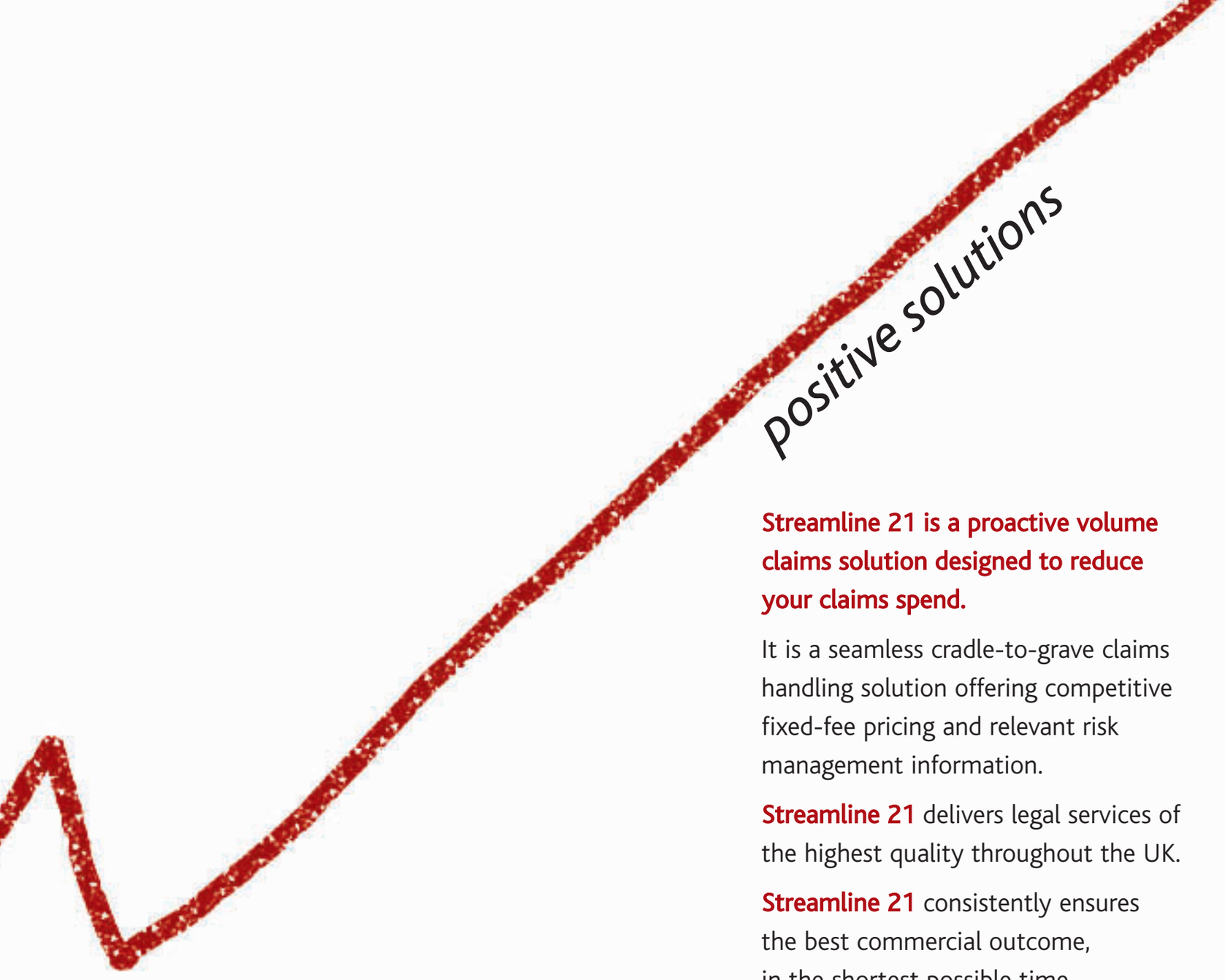
2007 EUROPEAN RISK MANAGEMENT AWARDS

StrategicRISK

BOOK YOUR TABLE NOW!

Held in the Brewery, Chiswell Street, London on April 18th 2007, the StrategicRISK European Risk Management Awards will recognise and reward excellence within risk management functions across Europe.

For table sales and general enquiries please contact: Claire McShane on +44 (0)20 7618 3417 or email: claire.mcshane@newsquestspecialistmedia.com
Tables of ten cost 3,800 euros (£2,500)



Streamline 21 is a proactive volume claims solution designed to reduce your claims spend.

It is a seamless cradle-to-grave claims handling solution offering competitive fixed-fee pricing and relevant risk management information.

Streamline 21 delivers legal services of the highest quality throughout the UK.

Streamline 21 consistently ensures the best commercial outcome, in the shortest possible time.
For a demonstration, please email:
philip.dicken@hughjames.com
or call: 029 2039 1071

www.hughjames.com

Winner of the Risk Management Product of the Year Award at the Strategic Risk 2006 European Risk Management Awards

streamline 21