CIR
CONTINUITY INSURANCE & RISK

In association with

Reputational risk and IT

IBM®

In association with IBM

A reputation to rely on

This roundtable was held to discuss the relationship between a company's reputation and its IT

Setting the scene

There is a clear shift in the use of technology that has been happening over a period of time. One result of this change has been that we are thinking less about "recovery", (and as a consequence, business continuity being provided on the basis of dedicated or syndicated server assets any more). Also virtualisation and provisioning technologies, both on their own and as part of the advent of cloud, challenge both commercial models and delivery operations in new ways. There is also a move towards technology needing to more regularly support a continuously available service.

DM: The fact that technology supports those new ambitions is interesting and exciting for IBM BCRS as a business as we work with our clients. Also, a subtle but important shift of underlying tone has taken place, which has permeated business, political and economic sentiment. In the five or six years since the financial crisis there has been a focus on resilient dynamism. This is about supporting a business strategy, growth, mitigating risk, and therefore it is about the actions of resilience, and about business continuity supporting a positive, revenue generating, profit generating, forward-thinking position.

CM: I was fortunate enough to join IBM BCRS at a point of change such that I am having different conversations based on technology concerns from those that might have taken place four or five years ago when we talked about traditional disaster recovery, and I'm interested to hear the views of everyone here in terms of what the market now looks and sounds like.

MD: I'd like to know how everyone here actually defines reputational risk because it is an abstract rather than a tangible risk. So, in terms of who carries ultimate responsibility, I would like to hear how people approach this.

BA: I am interested in both elements, given that recent high-profile outages within some UK banks have led to a focus on the associated risks. We need to focus on how exposed and how resilient our systems would be if that happened to us. From a reputational point of view, recent changes have led to a refocus of our values. We are now trying to look at reputation from the customer's point of view.

GB: We are in a market that has changed quite drastically from one that was really revenue dependent to one that is branching out into a lot more commercial activities. We are also a great deal more technology dependent. Our approach to business continuity, resilience and risk itself, has had to do some catching up.

PC: I am interested in cloud and social media risk, but particularly in what happens when the risk is realised and your reputation is all over the front page.

KS: We agree there is a major shift taking place in this market.

BB: We have a fairly conservative approach to continuity. It would take a considerable effort to convince management of the security of customer data in the cloud, for instance. It is quite difficult to sell to the board as a concept, as it is a challenge to say specifically where data is stored. We would suffer a massive reputational hit if we lost customer data. That would be something that would impact us all the way up to somebody having to go the regulator and explain in excruciating detail what went wrong and what we are doing to fix it, therefore reputational risk in that sense is extremely important to us in terms of securing data, and indeed any continuity solution we have. We have to make sure that that's a cornerstone.

GR: We would like to know about best practice in crisis management exercising following a data breach.

NC: I'm very keen to learn how reputational risk impacts beyond one's own organisation, on both the customer as well as the supplier sides. Just how in control do companies feel about the whole risk profile, and what needs to be done to get that under control?

VM: Before the financial crisis there was a dynamic that existed around corporate strategy and deal making: will it be commercially successful; is it consistent with our risk appetite for reputational risk; and will the regulators approve it? That's all changed now and I would like to see what the philosophical response is to that and as well what sort of risk frameworks are being applied.

CB: We are taking a proactive and more customer-based approach to resilience, thinking beyond traditional silos and looking at how we can better prevent the impact of failure in the first place. However, we also recognise that all organisations suffer failures so you need a strong capability to recognise this, cope with it and learn from these events when they do occur.

Attendees:

Chair: Deborah Ritchie	Editor	**CIR Magazine**
Banker A		**A financial institution**
Banker B		**A financial institution**
Curtis Baron	Group Head of Business Resilience	**RBS**
Gabriel Barrett	Group Head of Risk and Resilience	**Circle Anglia**
Pete Chenery	Director of Information Security and IT Governance	**Circle Anglia**
Matthew Dyckhoff	Executive Director, EMEA Business Continuity Management	**Nomura International**
Nick Kuhle	Sales Manager, Business Continuity and Resiliency Services	**IBM UKI**
Chris McBrayne	Director, Business Continuity and Resiliency Services	**IBM UKI**
Victor Meyer	Global Head, Corporate Security and Business Continuity	**Deutsche Bank**
Dan Murphy	BCRS Portfolio & Strategy Leader	**IBM UKI**
Gillian Randle	Risk and Business Continuity Manager	**LCH**
Kevin Stevens	Sales Manager, Continuity and Resiliency Services	**IBM UKI**

It is a never-ending task and a huge challenge in an increasingly complex world. It is as much operational as it is strategic and cultural.

How does robust IT underpin robust reputational risk management?

DM: Starting by looking at reputational risk management from an IT perspective can provide a good level of understanding of the interdependencies that exist and how those interdependencies maps across the organisation. This can provide a way of breaking down business or organisational silos and attaining senior leadership buy-in from the board by providing a joined up, end to end view in a smart way.

CB: Resilience must be driven from the customers perspective. Organisations need to understand what is critical to customers in order to help protect them from disruption. It's not just an IT issue. You need to consider how your people and supply chain support your key activities also. High availability organisations embed resilience top down as well as bottom up. We encourage our risk teams to challenge decisions. This is vital if you are going to build a culture that uses risk as a tool. Too many organisations treat risk as a process that must be complied with.

NC: How many other people here feel that they've got board level sponsorship to look at reputational risk and help you build it?

CM: I think there is a change in sentiment in the industry. It used to be about disaster recovery, but now it is more about reputational risk or the reputation built on the service you provide your customers, and technology is one of those key elements that supports that.

KS: Expectations are so different now. A few years ago, people would check their balance on a visit to a branch but now they may do so over the phone – many times a day. Transaction rates have grown enormously because of the availability of services, and customers have come to expect that level of service all the time.

CB: Meeting customer expectations in terms of availability is a challenge. Organisations need to adapt quickly. The exponential growth in

In association with IBM

Reputational risk roundtable

smart phone use is driving a re-think on how to communicate with customers – both when things are working well, but also when they're not.

KS: When an army of journalists are watching!

NC: How long would it take you to disprove a data breach?

CB: It's important to maintain a readiness to respond to any incident. Customers deserve open, honest and regular communication, even if you don't have all the answers they are looking for.

VM: I think people generally think they understand reputation risk but what they don't get are many of its key attributes. Besides being about what you do and do not do, it is also about public perception, and banks in particular miss this piece. What they have not recognised until recently is that it is the customers that are the most important, and that has raised the bar in terms of reputational risk mitigation and acceptance levels. You basically have three choices in managing risks – transfer, accept, or mitigate. Clients don't care if you've got insurance, as by that point it is too late as continuity risks can be franchise threatening. Accepting the risk is unacceptable because the risk appetite of the board for reputational risk is zero. So you essentially have to mitigate everything. The problem with reputational risk is that it cuts across all risk factors and so it's very difficult to put your finger on it. No model, no risk control self-assessment, no scenario planning, no use case analysis of any model is going to allow you to identify it. It requires different approaches, and that has to be enshrined in process and governance.

DM: It's very interesting you mention insurance because I am aware of conversations and have been approached by a number of people in the insurance industry keen to better understand and quantify reputational risk by putting values against it and building models to determine those values. At present they have allocated only a small amount of money across the whole of Europe to insure against the risk of reputational damage and as such these sums only realistically pay for lawyers in the event of an actual event resulting in reputational damage – which doesn't feel like an appropriate response.

VM: You have to self-insure, which, in other words, is mitigation.

BB: To explain reputational risk I would use the analogy of an engine, which has various bits and pieces in it representing the more tangible pieces of the risk, like credit risk, market risk, operational risk, and legal and compliance – all of which management understand, and reputational risk is the oil. It's the intangible thing that you never see quite working in an engine but without it the whole lot stops, and getting management to focus on the intangible nature of that and is the real trick to getting management to spend money on something that is intangible.

DM: But is it really that intangible?

AP: Yes though it seems more tangible now because there have been and there is a lot more focus through the media, where if something is going wrong it doesn't stay localised for very long, but blows quickly out of all proportion. Who would have thought Arthur Anderson would have been put out of business because they shredded documents and were found guilty of contempt in Congress? But that's what happened, and I'm sure none of their reputational risk people had ever cottoned onto the fact that somebody putting something in the shredder would effectively close them down.

VM: I just don't think that effectively managing reputational risk requires significant investment. I think it's much more about governance processes that are able to catch it early and react, or act extremely decisively to very weak signals, and be able to recognise and map dependencies very quickly and respond. I can have a great plan in place for any sort of IT outage. I can get somebody in front of a camera in 15 minutes. But it would take me hours to get someone in front of a camera if I was confronted with a similar scenario as happened recently at Zurich. I think this is about connecting the dots across all the various risk types and going deep into the business and identifying those key areas, stitching them together and being in a position to escalate issues very, very quickly.

Communicating reputation

MD: Is reputation risk management actually a name that exists in your company? It's very abstract and I think all other risks lead ultimately to reputational issues if you don't have the correct control mechanisms or resilience and crisis management in place. But it seems to me that you're saying there is actually a reputational risk management team, person or partner in the company. For me the executive board is responsible for reputational risk. It is about the strategic direction of the company. It depends on your company structure, but, ultimately it's within all the different risk and control areas of the company. Everyone has a level of responsibility and planning and corporate responsibility.

CM: Times have changed, and in a connected world where bad news travels so fast, and the media are waiting for something bad to happen, it makes something as abstract as reputational risk a much more relevant conversation. That's predominantly because it's about communication and how you manage that risk. It's about what you do once the event has happened and how you manage that, hence the importance of tackling social media risk. It is seeing that the person responsible for the response is the same person who is in charge of the management of the company's reputation, so it's really tangible, and very relevant.

MD: It's an integral part of risk management and our areas of responsibility, including my own. And there is a huge amount of pressure with an ever increasing amount of regulation. And ultimately everything comes back to IT in some form or other.

VM: We struggle with that as well and I think we are on the way to cracking it. The way we can contextualise it is that you're dealing with an area that sits in between crises and normal daily operations, and in normal daily operations everything runs fine, albeit with some minor issues, but in general they're managed within normal work structures. Where people struggle is when things go from normal daily operations into what we loosely would call an incident. They don't ask themselves, could this become an incident? Typically where we experience problems is when an issue deteriorates into an incident, but the organisational response is insufficient – issues tend to just sit there in a given division of business unit, and they try, (and IT is notorious for this) to fix the problem, but they don't see the larger context. They don't involve anybody else; they just focus on trying to fix a discrete problem while ignoring the second order effects. And so they continue to operate in their silo. What incident management is decisive multi-disciplinary action, acting on very weak signals, acting very early before an event does become a crisis, so you get the media team, technology, compliance, finance – everybody – involved, and reviewing cases on a weekly basis and when something looks like it could be problematic, decide to escalate that to regional management. Then if regional management doesn't like it, it's analysed and escalated in a well structured way. With any other approach, everything goes to the board and they're inundated. Therefore, you have to have a governance structure in place so decisions are taken at the right level, and incidents that aren't severe are managed more locally – and only escalated if necessary.

DM: The only way of containing the growing impact of incidents on reputation is putting the emphasis on preventing them from occurring in the first place. You're not just talking about the cost of downtime any more; you're talking about the compound costs of months and years of investment in building your brand.

VM: I agree to a point. One of the things that people don't get about reputational risk is that it has a half-life. Look at payment protection insurance. Regulators were fine with PPI until perceptions changed. It's really, really tough to go to an investment bank or any firm and say 'we should be looking at the things we did in the last five years that could bite us in the future'. Nobody can do that – it's too abstract. And that's why you have to be able to react.

CB: Prevention is better than cure, and I think it is about paying attention to the near misses. Firms need to shift leadership to the right point and ensure that decisions are taken with the customer in mind. In my view organisations need to mature their relationship with risk and ensure there are very clear accountabilities.

BA: One of the major things that we've done is try to assess all of the activities undertaken from the customer's perspective. This has changed what we perceive to be important

In association with IBM

Reputational risk and IT

and it's good to see the management taking that forward. That's what's spurring us on to actually drive how we become more resilient by doing the cheaper, easier elements first so not to spend money on infrastructure and technology where you can do the quick win by making sure functions are split geographically, and then look at the technology and supply chain afterwards.

BB: So who in the company carries out responsibility for reputational risk? Compliance functions are not risk functions in terms of owning what is, as I said, the "oil in the machine", and how that helps all of the other bits of the organisation function. Reputational risk has been left with compliance because nobody else has taken unitary ownership of it because to a certain extent it's a poison chalice.

The upsides

CB: While we never wanted our recent incident to happen in the first place, a lot of positives have come out of it. Organisations become galvanised during a crisis and actually it brings out the best in people. Indeed it even built bridges with our customers. The trick is to make sure you don't walk into the next disaster by then just focusing on what's just happened. I also got a lot of phone calls after that incident from industry professionals wanting to know what went wrong and how they could prevent it happening in their own organisations.

BA: One of the things that we done is encouraged more collaborative working, right down to the way the offices are being organised. By bringing management out of the office and creating something more akin to a Google campus, if you like, so you have division heads sat in a group, and that encourages greater co-operation. So, as opposed to saying 'this is my budget' or 'this is my bit', staff are now saying 'this is our budget'. This seems to be working for us so far.

VM: The financial crisis was incredibly cathartic because it forced banks to be incredibly introspective. The regulators are punishing us. Higher capital and leverage requirements, more focus on every area of risk and governance and it's driven some of the people that were short-term thinkers to completely rethink beliefs, values and behaviours.

The cloud

KS: There was a comment in our recent paper about robust IT on the movement towards cloud technologies. How do we assure robust IT with some of these newer technologies?

BA: When you look at the regulatory scrutiny in the financial sector, there is a big drive to learn from new and younger organisations. What we're trying to do is take what we can from new start-ups and see how we can best fit it into our culture an industry and make that work for us.

CM: The general perception of cloud is that it is public. The reality is that for our clients, it is much more dedicated and shared cloud environment with some of our solutions, but they're shared to a group of clients within our infrastructure or we have dedicated cloud depending on their needs. You can apply the same types of secure technology as you need to, but today you can access your data in a much cleverer way, to new RTOs.

BB: In fact, the two biggest information leaks on the planet had nothing to do with the cloud.

CM: The exponential growth in data usage is ridiculous, certainly in banking, and I'm sure in most organisations, so financially it makes a lot of sense to think about a virtual way around storing data securely.

NC: I think the perception around cloud, is that it's 'out there somewhere', that it's unsecure and the reality is that there's some incredibly secure cloud. Your own private clouds are as secure as if it were not called 'a cloud'. It is also about the ability to be agile and react quickly and provision quickly. An insurance company asked me this week to explain our Smart Cloud Managed Back-up, Virtual Server Recovery and our Smart Cloud Content Manager, as they were concerned about security in the cloud. And it's back to perception again... the perceived idea of what cloud is, is not necessarily the case.

PC: That's partly because of consumerisation.

Third party suppliers

KS: Tesco is a great example of how to respond to a crisis. They've even got a reputational bump on that.

VM: That's right, but it's interesting culturally because right after that happened consumption of horse meat in France doubled. It's all about cultural perception. Take the deeply ingrained concept of spying on the German psyche, which means the regulators are extremely rigorous on forcing vendor risk management standards to make sure that inappropriate data disclosure doesn't occur through third parties. Some of the smallest vendors pose some of the biggest reputational risks.

CB: Understanding the resilience risk across your critical supply chain is a strategic imperative. One of the key areas of shared concern across our sector is the security of data held by legal firms.

DM: We've had a number of conversations with legal firms around the disposal of data and the majority have mentioned that up to this point they had a policy where they simply don't dispose of any data at all.

Risk culture

NC: Do we think there is no way to mitigate against every type of risk and that it comes down to how do you manage it once it happens?

DM: I am not sure I agree. With the recognition of and actual impact of reputation becoming bigger and more significant – it means the balance around prevention versus cure is shifting more and more towards preventative measures. Also the balance you take to applying these preventative measures needs to be considered carefully. For example, it is unlikely you can adopt a security policy, implement security tools, and apply supporting processes and delivery functions that will 100 per cent prevent some of the more planned and well sponsored security threats that exist today. So you need to balance an appropriate and reasonable security response with an adequate resiliency solution – while ensuring your business is resilient is becoming more and more important at all levels. Our reputational risk study shows potentially up to 21 per cent of a company's brand value is at risk through a data breach. You need to be in the business of prevention rather than cure, and prevention is about resilience first with a well considered security posture supporting this resilience posture. You can secure against the recreational hacker, you can't secure against the well organised, well sponsored and determined hacker so you must have a seamless plan B. That is how I would sum it up.

BA: Resilience is really key in our world. That's where we want to be and we have good buy-in achieve that. We are starting with aspects that are small and easy to achieve, and will go from there.

CM: Is it easier getting buy-in today than it was, say, five years ago?

DM: So being slightly controversial, is it about making money or is it about being good corporate citizens?

CB: First and foremost we exist to protect the customer, and in doing so, you protect the bank. We have a duty not just to ourselves but to society and the economy we support.

GB: But how do you get that shift in culture from focusing on the organisation to focusing on the customers?

CB: One of the hardest things to change is culture and our industry is also going through this. It's a difficult journey but long overdue.

VM: I actually believe negative incentives work better than positive incentives. There are two mechanisms that are kind of yin and yang. One actually diffuses accountability, the other one concentrates it. The one that diffuses it is governance. We are a German bank so we love consensual decision making: get a big group of people in a room and everybody gets to talk about it. It's not very efficient, but it does connect the dots and meeting notes have a way of focusing the mind. The other side is risk acceptance. So if you and the board define your risk appetite in a particular area and you accept the residual risk, to a as low as reasonably practicable (ALARP), and accept the differential, it's the individual risk owner that accepts that. And if then the event happens, if that's effectively linked back to bonus call back or results in a red flag, you start to hold people individually accountable for negative outcomes, which really focuses the mind. I've seen some incredibly interesting conversations occurring, and actually less risk is taken, and it prevents you from backing into risk as you can't squirm out of it. The risk owner owns the risk and the governance structures are there to enforce that accountability.

Implications of the IBM Global Reputational Risk and IT Study

In 2012, we reported what more than 600 executives in 23 countries told IBM about reputational risk and IT risk. In 2013, we offer practical advice about preventing and mitigating those risks.

Keep an eye on reputational risk and IT in 2013

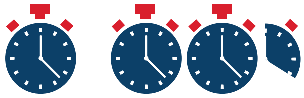
From password hacks and cyber theft to a highly visible system outage or a full-blown disaster, you are more exposed than ever to IT-related risks. What's most at risk is your company's reputation—and ultimately your bottom line. It's never been more important to take the steps that can help you protect your reputation.

What is the cost?

-21%

The true price of reputational harm

The economic value of a company's reputation declines an average of 21% as a result of a breach of customer data.[1]



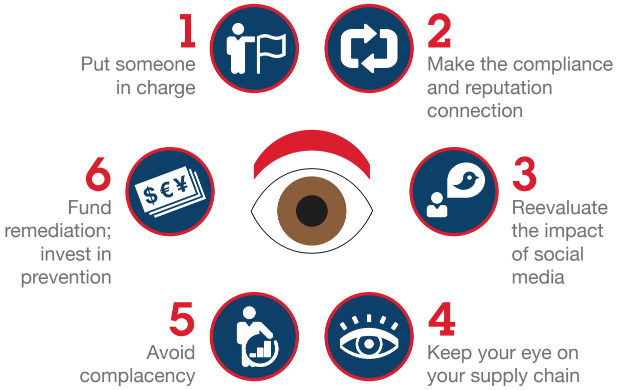
$181,770 per hour

$418,017 per event

The cost of system downtime

The cost of an hour of data center downtime for an industry-average organization is $181,770. Most business interruption events last on average 2.3 hours.[2]

What should you do?



1 Put someone in charge

2 Make the compliance and reputation connection

3 Reevaluate the impact of social media

4 Keep your eye on your supply chain

5 Avoid complacency

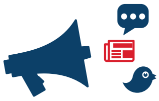
6 Fund remediation; invest in prevention

Consider a new dimension...

Add a third dimension to risk management

In the past, risk management decisions were based on the likelihood of the event happening and its potential impact.

In today's connected world, a third dimension—velocity—can have the most impact on reputation. With social media and the web, stakeholders know about negative incidents almost immediately.

1	Likelihood	1 in 7? 1 in 100?
2	Impact	Severe Moderate Mild
3	NEW! Velocity	

Watch for the rise of the Chief Digital Officer

As digital becomes part of every corner of your business, the skills of a Chief Digital Officer will bring a focus to how your digital presence can help build and protect your reputation.

How well are you doing?

Rate your ability to protect your reputation in 2013

Find out how your organization compares to our benchmarks. Answer a few easy questions and the online IBM Reputational Risk Index will score your efforts.

Start protecting your reputation from IT-related risks today

Read the paper
Six keys to effective reputational and IT risk management
ibm.com/services/riskstudy/uk

Find out your score
IBM Reputational Risk Index
ibmriskindex.com

[1] "Reputation Impact of a Data Breach: U.S. Study of Executives & Managers,"Sponsored by Experian® Data Breach Resolution Ponemon Institute, November 2011.
[2] "Datacenter Downtime: How Much Does It Really Cost?," Aberdeen Group, February 2012.