# What if…?
# Exploring attitudes towards risk

**Circle**research

# Contents

# The people behind it

### Carolyn Williams, Head of Thought Leadership, The Institute of Risk Management

Carolyn Williams MA ACII MIRM is Head of Thought Leadership at the Institute of Risk Management, the leading international educational and training body for the risk management profession. Thought leadership involves tracking what's going on in the world of risk management and bringing it back into the Institute's publications and events, and also communicating the work of the Institute to the wider world.

Carolyn joined the IRM in 2006 from Lloyd's of London, where she was responsible most recently for risk management training and communication. She is also a member of the Chartered Insurance Institute's Qualifications, Examinations and Assessments Committee and of the Advisory Board for Nottingham University's Centre for Risk and Insurance Studies.

### Andrew Dalglish, Director, Circle Research

Andrew has specialised in B2B research for over a decade and co-founded Circle Research in 2006. He is a columnist for B2B Marketing Magazine, a frequent speaker at leading events such as the Social Media World Forum and teaches the MRS B2B research course.

Andrew holds an Honours degree in Psychology from Aberdeen University, an MSc in Marketing from Strathclyde University and the MRS diploma.

### Petra Wilton, Director of Policy & Research, The Chartered Management Institute

At the CMI, Petra Wilton takes a lead role in building partnerships in the public policy arena and promoting the needs of practising managers through engaging with and accessing the views of the CMI's 90,000 members. Through a bespoke research programme and policy initiatives, these views are shared with those in Government, business, education and the media.

Petra manages the All Party Parliamentary Group on Management and represents the Institute on various external groups including the Department for Business, Innovation and Skills' Management and Leadership Network Group and Professions for Good.

Petra has an MA (Hons) in History from Cambridge University and is a Fellow of the RSA.

### Lee Glendon, Head of Research & Advocacy, The Business Continuity Institute

Lee Glendon is Head of Research & Advocacy at the Business Continuity Institute, the leading institute for Business Continuity Management practitioners with over 7,000 members in more than 100 countries. Lee holds the Certificate of the BCI (CBCI) with merit and is author of a number of studies on the future of risk management, and supply chain resilience. Prior to the BCI, Lee worked in the telecoms sector for 10 years in the UK and Germany working across innovate start-up ventures and major blue chips.

### Roger McLoughlin, Business Continuity Manager, Vodafone UK Ltd

Roger joined Vodafone UK in 2001. His responsibilities include managing the implementation and maintenance of Business Continuity and Crisis Management across Vodafone. He is also a consultant on Business Continuity best practice to the Vodafone Global Business Continuity and Risk community. As a result of his work, Vodafone UK was the first Mobile Telecommunications company in the world to achieve certification of BS25999 for its network and subsequently also won Business Continuity strategy of the year at the prestigious CIR Business Continuity Awards 2009. Roger is a well respected figure in Business Continuity and has had articles published in The Journal of Business Continuity and Emergency Planning, The Forrester Report and Talking Business Continuity. Roger is a member of the Business Continuity Institute where he is also a membership assessor.

# Preface

We're waking up to risk.

Business Continuity as a profession began as far back as the 1970s when engineers looked at developing reliable methods to recover lost data if their mainframe computer suffered a 'disaster'. They coined the term "Disaster Recovery".

Since then business continuity has been on a journey of evolution that still continues today.

One of the first major developments was the realisation that if disaster recovery planning could help protect valuable mainframe computers, then this could be applied to other areas of the business. This holistic approach became known as Business Continuity Management (BCM).

Recent developments in BCM have focused on integrating different aspects of continuity and developing best practices. This has led to the recently launched International Business Continuity standard, ISO22301, which Vodafone is proud to be piloting.

The pages which follow reflect this growing awareness of risk and response. It's encouraging to see that many have now adopted the principles of business continuity planning. More encouraging still is that these plans are viewed as valuable, practical tools rather than a 'tick box' exercise.

When reviewing our own business continuity plans here at Vodafone, we ask questions that might act as a useful companion when you browse this report:

- what are the most critical things that we need to protect?
- as a business, what is it that we do and what could cause this to stop?
- what actions do we need to take should the worst happen?

# Landscape of risk

Organisations have always been vulnerable to myriad risks. However, in recent years, the risk landscape has changed both in nature and our attitude towards it.

As business leaders we're much more conscious of the threats faced and how they can hit us when least expected. The collapse of Lehman Brothers in 2008 and the ensuing financial crisis brutally reminded us of this.

But fundamental change in the risk landscape was brewing long before the Lehman incident. Technology has liberated and enabled us, but at the same time has created a new category of risk. The interconnected, globalised world in which we now live has made risk more complex and the repercussions of an incident harder to predict. At the same time there's been no respite from 'traditional' risks like natural disaster, civil unrest and pandemic.

This second report in Vodafone's **Perspective series** explores how UK organisations view and respond to risk. It answers questions such as:

- where does risk management sit on the organisational agenda?
- what risks do organisations fear most and how are they responding?
- what role does technology have in creating and responding to risk?

Our aim in producing this report is to help organisations find better ways of working and enhance your business planning and operations. As with other reports in the Perspective series, the guiding principle is to strike a healthy balance between opinion and fact, theory and practice, observation and advice.

At the core of the analysis is a primary research survey commissioned by Vodafone. Conducted by Circle Research in October 2011, the survey canvassed the opinion of 615 senior managers in small (1-99 employees), medium (100-499) and large (500+) UK organisations across the public and private sector.

The findings are further complemented with selected extracts from the Chartered Management Institute's (CMI) 2012 Business Continuity Management survey and a closing chapter written by the Institute of Risk Management (IRM) which explores the future of risk.

We hope you find the report interesting reading and explore the resources available at **www.vodafone.co.uk/perspective**

"It's important to consider all risk and disruption have business consequences such as loss of revenue, increased costs or even reputational damage.  But even if no disruption occurs, organisations can use Business Continuity Management to demonstrate that they are a well-managed business – this brings other benefits such as a  better credit rating and lower insurance premiums"

LEE GLENDON, HEAD OF RESEARCH, THE BUSINESS CONTINUITY INSTITUTE

# Executive summary

### Key findings
This report reveals that:

- the organisational focus on risk is intensifying
- management perceive two tiers of risk, with technology threats topping the list, followed by talent and environmental risk
- technology is also seen as a solution to rather than just a cause of risk
- organisations recognise that employees are critical to commercial success
- the probability of talent-related risks occurring, such as defection, is relatively high
- despite this, preparations to counter talent risk are relatively weak when compared to other threats

### Waking up to risk
Three fifths of UK managers report that their organisation has become more focused on risk in the last three years. In larger organisations this is reflected in the widespread adoption of business continuity plans. Nine in ten organisations with over 250 employees have such plans and they are especially prevalent in three sectors: Finance, Healthcare and the Public Sector.

This is far from a 'tick box' exercise. Plans are kept fresh, with over 75% updating them in the last year. Plans are also kept effective, with three fifths testing their plans in the last year.

However, whilst more common than not, business continuity planning is still far from universal. Just two fifths of organisations with up to 10 employees have continuity plans in place. This rises to four fifths in those with 50-249 employees. Two reasons underpin this lower adoption rate: a lack of resources and a belief that the nature of risks faced doesn't justify such a plan.

### The two tiers of risk
Risks can be categorised into two groups – tier one and tier two – based on the level of concern they cause management. Of greatest concern is technology-related risk, being a tier one risk. 59% of managers are concerned about IT systems failure, 46% worry about telecommunications system failure and 39% fear hacking attacks.

Behind this come tier two risks:

**Talent risk** threats to an organisation's talent pool, e.g. defection to competitors, illness

**Environmental risk** threats posed by 'acts of God', e.g. natural disaster, adverse weather

"Managers may feel they have all their bases covered when it comes to their own organisation's business continuity management, but in a global economy few firms are insulated from disruption to their suppliers, distributors and customers. This means managers need to work with their business partners to ensure the complete value chain is not only resilient to disruption, but better placed than the competition to take advantage of others' failure to plan for the worst"

LEE GLENDON, HEAD OF RESEARCH, THE BUSINESS CONTINUITY INSTITUTE

Talent risk is slightly higher up the management agenda than environmental risk but far behind technology risk. For example, the most likely cause of permanent employee loss – defection to other organisations – is of significant concern to just 29% of UK management. This disconnects with the high probability of such events. The average employee rates their job satisfaction at a lacklustre 6.6 out of 10. One in five are actively considering moving job in the next 12 months.

Likewise, the CMI Business Continuity Management survey shows that disruption caused by extreme weather is the most common risk event experienced by UK organisations. However, just one quarter in our survey saw environmental risks such as adverse weather as a significant concern.

### Technology – a source of risk, but also a solution
Whilst technology is on the one hand, a source of risk, organisations acknowledge that it serves to protect them against the more 'traditional' tier two risks.

Firstly, technology reduces the disruption from environmental events. One half of organisations with business continuity plans in place indicate that mobile technology forms a prominent part of these. Two fifths report the same for remote access to IT systems.

Secondly, technology can mitigate talent risk. 50% of organisations believe that access to flexible working has become more important in determining employee satisfaction. Indeed, one fifth go so far as to name flexible working as one of the top five determinants of employee satisfaction.

### Advice from the Institute of Risk Management
In their closing comment to this report, the Institute of Risk Management (IRM) provides four pieces of advice for those looking to better manage the risk inherent in our world:

1. not all risks are obvious. Take a systematic look at events that might stop you achieving your objectives
2. although some risks seem improbable, the event can happen. There are usually steps that you can take to prepare for the worst
3. make solid business continuity plans for when things go wrong
4. make sure you're taking all the steps possible to ensure things go right in the first place

Applying this philosophy requires skill in risk management but it also goes hand-in-hand with general business excellence – organisations that are good at managing their people, their systems and other aspects of what they do, tend to be good at managing their risks too.

"Over the past 30 years we have seen the way we organise our work and our lives changing in response to new technology. This is going to continue. Each wave of change brings both benefits and risks and we need to make sure we're tackling the issues of today and tomorrow, rather than yesterday. Even if we're more comfortable with yesterday!"

CAROLYN WILLIAMS, HEAD OF THOUGHT LEADERSHIP, THE INSTITUTE OF RISK MANAGEMENT

# Waking up to risk

### AT A GLANCE

**1**. The focus on risk is intensifying. 61% have become more focused on organisational risk in the past three years.

**2**. This focus is coupled with greater preparedness. 91% of large organisations (250+ employees) now have business continuity plans in place.

Recent years have seen a plethora of risks turn to reality.

The devastation that natural disaster can bring was painfully demonstrated in the 2004 Indian Ocean tsunami which claimed thousands of lives. The catastrophe which ensues when natural and man-made risks collide was seen in the Fukushima nuclear meltdown triggered by a tsunami in 2011. And the consequences of excessive financial risk were illustrated in 2008 by the collapse of Lehman Brothers and the subsequent unravelling of our financial system. All these events have had significant human and economic impact.

But risk is nothing new. Take financial risk as an example. Flick through history books and it's a recurrent theme: the Dot Com Bubble (2000), the Great Depression (1929 – late 1930s) and Tulip Mania (1637).

You'd think we would have learned our lessons long ago. However, it's only in relatively recent times that organisations have begun to seriously address risk. The role of Chief Risk Officer (CRO) only became a formal position in 1993 with the appointment of James Lam as CRO at GE Capital[1]. And the first International Risk Management Standard – ISO 31000 – was published just three years ago in 2009.

We've slowly been waking up to risk and the focus is now intensifying.

Our survey of 615 senior managers in UK organisations reveals that 61% have become more focused on risk in the last three years. And not just focused, but prepared.
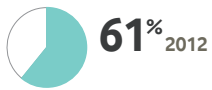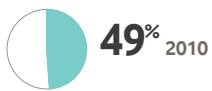
1 'Organizational Encounters with Risk'.  Bridget Hutter and Michael Power.  Cambridge University Press.

ADOPTION OF BUSINESS CONTINUITY
PLANNING IN ORGANISATIONS

**61**%
**More focused on risk
in last 3 years**

**26**%
**Instigated plans
in last 2 years**

**58**%
**Tested plans in last
12 months**

BUSINESS CONTINUITY PLANNING
HAS BEEN ON THE INCREASE

**49**% 2010

**58**% 2011

**61**% 2012

### Preparing for risk

Business continuity planning – the systematic identification of threats facing an organisation and development of plans to recover should they occur – is now the norm in larger organisations. Nine in ten organisations with over 250 employees have business continuity plans in place. This formal response planning is particularly prevalent in certain sectors. All but a handful have business continuity plans in the Financial Services (95%), Healthcare (94%) and the Public Sector (93%).

26% of those with business continuity plans in place only instigated them in the last two years. This echoes a study by the CMI, which has tracked the adoption of such plans over the last decade[2]. In 2010, 49% of UK organisations had business continuity plans in place. Just two years later, this figure has soared to 61%.

It's also apparent that this planning is far from theoretical or a 'tick box' exercise.

Plans are kept fresh. Of those in our survey with business continuity plans, three quarters have updated them in the past 12 months. And they're kept effective. Three fifths have tested their business continuity plans in the last year. A further fifth have done so within the last two years.

So risk has clearly shifted up the organisational agenda in recent years and a new attitude seems to be emerging: risk management is being taken increasingly seriously.

But what exactly is it we're so fearful of?

# Weighing up the risk

**AT A GLANCE**

**1**. Risk falls into four categories: financial, strategic, operational and hazard. Within this, operational and hazard risks can be categorised as tier one or tier two based on the level of concern they cause management.

**2**. Tier one risks are all technology related.

**3**. Tier two risks are environmental and talent related.

The risks facing an organisation are varied. The IRM categorises them into four broad groups:

- financial risk, e.g. non-payment, cash flow
- strategic risk, e.g. entry of a new competitor into the market
- operational risk, e.g. supply chain failure, loss of key employees
- hazard risk, e.g. natural events, health & safety incidents

Not all of these risks are equal. They differ in the extent to which they can be mitigated and their impact, should they occur. Importantly, they also differ in their probability. According to the CMI, the five negative events most commonly experienced by UK organisations in 2011 were operational or hazard-related:

- disruption from extreme weather (49%)
- loss of IT systems (39%)
- loss of people (34%)
- loss of telecommunications (24%)
- industrial action (22%)

Of course, reality and perception don't always concur, so in our survey of UK management we wanted to explore which risks caused them greatest concern.

Their response suggests that, perceptually at least, risks fall into two categories – tier one and tier two – based on the level of concern management attach to them.
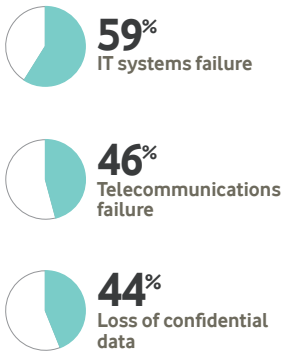
### Tier one: technology risk
UK managers indicated that their biggest fears, their tier one risks, were technology driven.

Of greatest concern to organisations large and small is the failure of IT systems. Three fifths of organisations reported that this was a significant concern. In a similar vein, telecommunications failure (46%), the loss of confidential data (44%) and hacking attacks (39%) were also cited as significant concerns.

This nervousness is understandable. Modern organisations are dependent on technology. For example, in April 2011 Amazon hit the headlines as the cloud hosting service it provides to other web businesses suffered a major, multi-day service failure[3]. High profile customers including Foursquare and Hootsuite were left counting the cost as they were unable to deliver their own services which rely upon Amazon's cloud infrastructure.

3 'Web chaos as Amazon cloud failure crashes major websites'. The Daily Mail, 22 April 2011.

TOP THREE OPERATIONAL RISKS BY
ORGANISATIONS

**59%**
IT systems failure

**46%**
Telecommunications
failure

**44%**
Loss of confidential
data

However, not all technology risks are so highly prioritised. Only 19% of managers see smartphone theft as a significant concern. Smartphone viruses (12%) and tablet viruses (13%) are also relatively minor concerns. Despite widespread use of these devices. The majority (56%) of organisations now enable flexible working, often with a smartphone or tablet component, for most employees. And with these devices holding or providing access to commercially sensitive information, represents a real risk. It's estimated that 100,000 mobile devices are lost on public transport every year[4].

## Tier two risks
Tier two risks are those which managers are less concerned about. Perhaps they're seen as lower probability. Maybe their impact is believed to be less dramatic. Whatever the reason, they're on the periphery of the management risk radar.

Tier two risks come in two forms – environmental risk and talent risk.

### Environmental risk
In February 2009, it's estimated that snow stranded up to 20% of the UK workforce at home. The Federation of Small Business estimated that the disruption cost the UK economy up to £1.2 billion.

As 2009's snowfall demonstrated, events in nature can have a huge impact on an organisation. Pandemics, adverse weather and similar events can severely disrupt operations and damage key facilities. Moreover, as the CMI's study reveals, disruption caused by extreme weather is the most common risk event experienced by UK organisations.

However, when taken alongside other risks, just one quarter of UK managers in our survey saw adverse weather as a significant concern. Perhaps because of the logistical challenges a bigger workforce brings, larger organisations are more likely to express such concerns than smaller businesses. Natural disasters cause a similar level of concern. One third expressed significant concern about long-term damage to key facilities through fire, flood or similar events. Slightly higher up the list is man-made destruction.

So environmental risk isn't currently of widespread concern. As we'll see shortly, this is perhaps because organisations feel relatively well prepared to deal with such events.

4 Vodafone and The Ponemon Institute. June 2010.

3 MOST COMMONLY EXPERIENCED
RISK EVENTS

**49**%
**Extreme weather**

**39**%
**Loss of IT systems**

**34**%
**Loss of people**

**Talent risk**

With the vast majority of our GDP being created by the service sector, the UK is without doubt a people economy.

As the first report in the Perspective series: 'Exploring the Shift in Employee Expectations' highlighted, for the majority of organisations, getting the best employees is central to their success. Indeed, eight in ten describe having the very best people as not just desirable, but critical.

It is remarkable then that 'talent risk' isn't at the top of the management agenda. Rather, it is of slightly greater focus than 'environmental risk' but far behind 'technology risk'.

The most likely cause of permanent employee loss is defection to other organisations which is of significant concern to just 29% of UK management. The most prevalent temporary cause of employee loss is illness, be it regular or pandemic, sitting at 28%.

Another temporary disruptor, industrial action, is cited as a significant concern by only 17%. In the heavily unionised Public and Transport Sectors, this rises to 35% and 26% respectively.

So despite talent being as critical, if not more critical, to organisational success as technology, it's far lower down the agenda. And although employee loss is far more probable than natural disaster, in a risk context they're of roughly equal concern.

Maybe the UK workforce is so motivated and loyal that employers have no reason to be concerned?

Well, no. Our previous Perspective report on employee motivation shows that the average employee rates their job satisfaction just 6.6 out of 10 and one quarter should be actively considering switching jobs in the next 12 months.

# The risk field

All may seem calm outside, but your organisation is under constant threat.

At any time a technological or environmental incident can strike. The rug can be pulled from underneath you by changes in the market like the emergence of a substitute product. Even your own employees represent a risk either through acts of commission (e.g. defection to competitors) or omission (e.g. negligence).

Fear not though, with adequate defences such as regularly tested business continuity plans, your threat can be significantly reduced.



## Environmental risk

LEVEL OF CONCERN TO ORGANISATIONS

**36%** Damage to facilities through fire, flood

**24%** Natural disasters
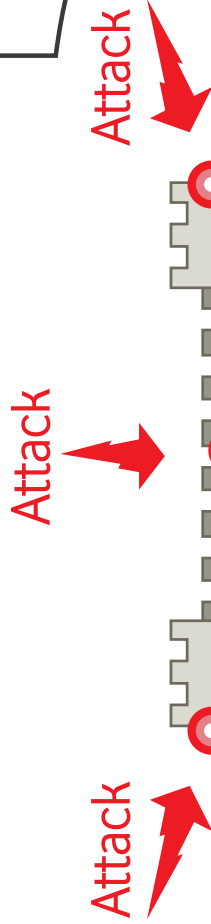
**23%** Adverse weather

## Talent risk

LEVEL OF CONCERN TO ORGANISATIONS

**29%** Defection to other organisations

**28%** Pandemic/illness

**17%** Industrial action

## Technology risk

LEVEL OF CONCERN TO ORGANISATIONS

**59%** IT systems failure

**46%** Telecommunications failure

**44%** Loss of confidential data

## Enemy within

**70%** of data breaches involve insider negligence

**30%** of incidents involve malicious acts

Financial risk

Strategic risk

Attack

Attack

Attack

## The defences

Of those with business continuity plans:

**76%** have updated them in the last year

**58%** have tested them in the last year

Of those with business continuity plans:

**52%** indicate mobile technology forms a prominent part

**44%** indicate remote access to IT systems forms a prominent part

vodafone

# Taking the risk

## AT A GLANCE

**1**. Business continuity plans generally reflect the relative concern attached to risks.

**2**. An imbalance seems to exist in preparations for tier two risks. Talent risk is of higher probability than environmental risk. Despite this, organisations are better prepared for environmental incidents than talent loss.

**3**. Technology also emerges as a solution too, as well as source of risk. 52% indicate that mobile technolgy form a prominent part of business continuity plans. 44% report the same for remote access to IT systems.

So, where they do exist, do business continuity plans focus on the risks most feared?

The answer is: mostly.

### Technology – a source of risk, but also a solution

As one would expect, tier one technology risks have the most robust continuity plans in place to deal with them.

Nearly one half of those expressing concern about IT systems failure describe their plans to respond as robust. A similar proportion uses this phrase to describe preparations in relation to hacking and data loss or theft.

It's also of note that whilst technology is on the one hand, a source of risk, organisations acknowledge that it serves to protect them against the more 'traditional' tier two risks.

Firstly, technology reduces the level of operational disruption from environmental events like adverse weather, civil unrest or pandemic.

Just over one half of organisations with business continuity plans in place indicate that mobile technology forms a prominent part of these and two fifths report the same for remote access to IT systems.

Indeed, in some sectors remote IT access forms the bedrock of business continuity planning. Three fifths of financial services and technology organisations describe its role as prominent. Contrast this with the retail sector where remote access is simply irrelevant for the vast majority of job roles.

Secondly, technology can help mitigate talent risk.

One half of organisations believe that access to flexible working has become more important in determining employee satisfaction. Indeed, one fifth go so far as to name flexible working as one of the top five determinants of employee satisfaction.

TECHNOLOGY FORMS A PROMINENT
PART OF BUSINESS CONTINUITY PLANS

**52**%
**Mobile technology**

**44**%
**Remote access to
IT systems**
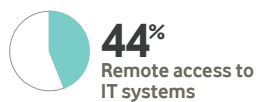
Given this context it's perhaps unsurprising that the majority of organisations (56%) now widely enable flexible working.

These employers also recognise the impact of flexible working on organisational performance and the bottom line. Flexible working is felt to create a more productive organisation (57% cite as top five benefit), enable a more flexible workforce (50%) and generate cost savings by reducing the requirement for office space (54%). In other words, flexible working is one risk that undoubtedly brings reward.

## Talent and environmental risk – an imbalanced response?

An interesting juxtaposition emerges when preparations for talent risk are contrasted with those for environmental risk. The former has higher probability. Employees are more likely to defect or become ill, than for freak weather to occur. Despite this, organisations are better prepared for environmental incidents than talent loss.

Amongst those concerned about employee defection to competitors, only one in ten have robust plans in place to respond to this threat. Three times that number describe their preparations as weak. Likewise, a mere 12% feel prepared to respond to the loss of several employees in one event; 40% admit plans are weak. Preparations to cope with employee illness are somewhat better, but still lacking. 20% believe plans are robust, whereas 24% weak.

Contrast this with preparations for environmental risk which seem far more solid:

- 37% describe plans for the loss of key facilities through fire, flood or similar event as robust
- 33% feel well prepared to respond to natural disaster
- 24% claim the same for adverse weather

Perhaps it's worth dusting off your own business continuity plans and asking whether they reflect the most pressing risks to your organisation's future?

"The business continuity benefits of allowing employees to work remotely don't usually feature highly in the decision to implement flexible working. Its value as a BCM strategy however becomes all too obvious when people face difficulties getting into work"

ROGER MCLOUGHLIN, BUSINESS CONTINUITY MANAGER,
VODAFONE UK

Putting into practice: The Yearsley Group

# Mitigating risk

The UK Federation of Small Businesses estimates that the heavy snowfall at the beginning of February 2009 cost the country £1.2 billion, with one fifth of the workforce staying at home due to bad weather. But for many it was business as usual thanks to a combination of mobile phones, mobile broadband, email and plenty of ingenuity.

Even though most people were aware that snow was expected during the night of Sunday 1 February, many were still astonished when they looked outside in the morning to see the heaviest snowfall in 20 years.

Although disruptive, the wintry weather also revealed the UK to be a nation of mobile workers, keen to get on with the job, without missing the opportunity for a bit of fun and a snowball fight.

Ged Tod felt a shiver run up his spine as he stepped into his office that Monday morning. As the IT Manager of The Yearsley Group, Ged is responsible for the technology infrastructure that supports the logistics operations of his organisation, which delivers frozen food to major retailers across the UK.

When he arrived for work, he discovered that three of his team were stranded at home. "We rely on the technology in our delivery centres and lorries to track deliveries and confirm delivery times. The bad weather could have had a catastrophic impact on customer relations".

Although many of the main roads in the country were open, even on the Monday morning, there were inevitable delivery delays as drivers were held up getting to work. Ged explains how technology helped put customers' minds at ease. "All our cabs are equipped with mobile phones and the lorries are fitted with GPS systems. It meant that drivers and employees in our call centres could keep anxious retailers up to date with the latest delivery times. Most of our customers were happy as long as they had clear and accurate information about when the goods would arrive".

Mobile technology also helped Ged manage his own team in Manchester. Two developers and one member of the support staff were out of the office for most of the week but used USB modem sticks to keep connected with colleagues. The absent member of the support team picked up helpdesk requests that could be dealt with remotely.

"Without this technology we could have lost close to 10 employee days that week".

GED TOD, IT MANAGER, THE YEARSLEY GROUP

# A closing thought from the
## Institute of Risk Management

No organisation can exist without engaging with risk, for without risk there is no progress and no reward. The future will inevitably bring more change and organisations need to identify and address the risks that this will pose for them.

This report has put the spotlight on technology – the risks it brings and the solutions that it provides – and also highlights the real, but sometimes underestimated, risks of losing talented employees. It has also emphasised that organisations of all sizes will need to become more resilient, with effective business continuity plans in place, to be able to bounce back quickly from misfortune.

We believe that research like this is important because it draws attention to risk areas that people may not have thought about fully before – they may believe that it can't happen to them (it can) or they may believe that there's nothing they can usefully do about it (but there usually is).

Once organisations start to think about what might happen, we recommend that you take a systematic and comprehensive look at all risks across your organisation that might stop you achieving your business objectives. You should ensure staff and advisers are suitably qualified and experienced to help with this. As well as making business continuity plans for when things go wrong, and using the most suitable technological tools and techniques available to do this, there is also a lot that organisations can do to ensure things go right in the first place. This requires skill in risk management but it also goes hand-in-hand with general business excellence – organisations that are good at managing their people, their systems and other aspects of what they do tend to be good at managing their risks too.

irm
Leading the risk profession