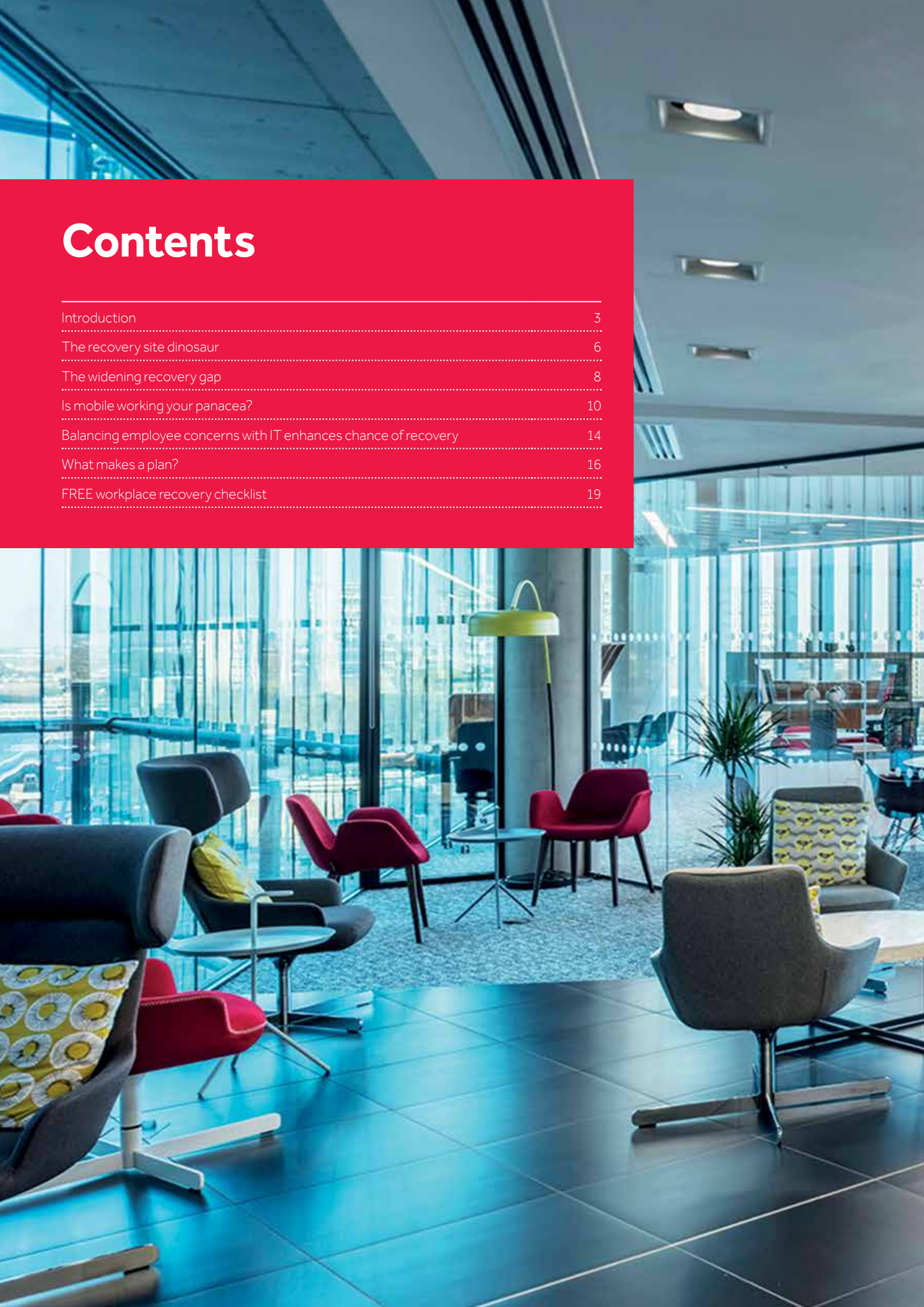
January 2016

How to protect your business from a catastrophe.

Why business continuity plans must consider the needs of people

regus.com/workplacerecovery

Regus™



Contents

Introduction.

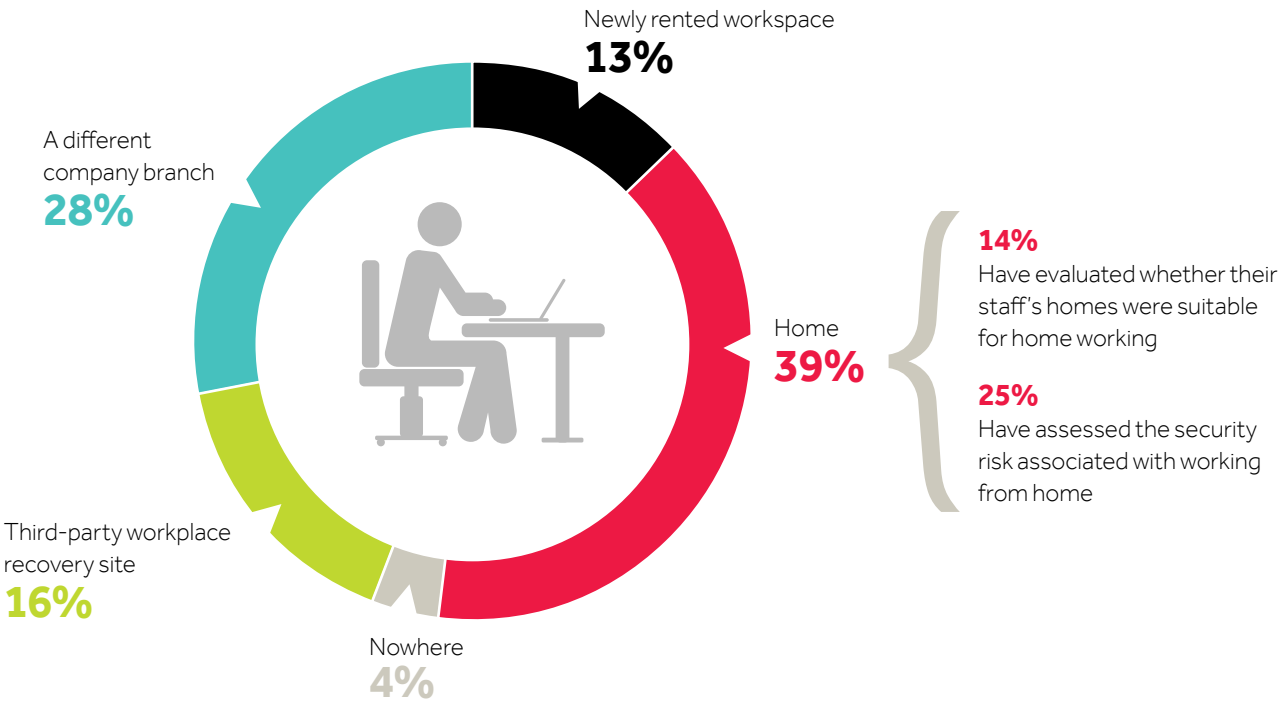
Despite all our best efforts, disasters do happen. Your company's ability to ensure that employees retain a working environment in which they can access critical data, applications and operations is crucial to its continuity.

Many think they are prepared, or can get by, but it is crucial to remember that dealing with a disaster well wins the loyalty of your customers; dealing with it badly can put you out of business.

When Superstorm Sandy ripped through the east coast of the US in 2012, the US Chamber Foundation's Business Civic Leadership Center estimated that 60,000-100,000 small businesses were negatively affected. Some 30 per cent of them were expected to fail within months as a direct result of the storm, according to a report by Forbes. It was also discovered that 52 per cent of businesses lost sales or revenues and almost half were forced to cease business for at least one week, with 71 per cent losing power for at least one day. As a result, 65 per cent said that they had customer issues because of Sandy, while 47 percent had employee issues and 44 percent had supplier issues. A National Hurricane Center report concluded: "Severe damage to small firms occurred in New Jersey, with nearly 19,000 businesses sustaining damage of $250,000 or more. Total business losses are estimated at $8.3bn." [1]

In March 2011 Japan was hit by an earthquake, which affected 740,000 small businesses, and a tsunami, which took out 80,000 companies. While no

Where will your staff work during a disaster?



“During the past 30 years, companies have realised the value of having a disaster recovery plan that includes fully equipped alternative premises to work from.

price can be put on the human losses, conservative estimates suggested that the disaster displaced more than 300,000 employees across 715 industries, costing $209bn in lost sales. As a result of widespread devastation and due to a lack of planning by businesses themselves, the Organisation for Small and Medium Enterprises and Regional Innovation in Japan arranged for temporary offices to be leased to SMEs via municipal government bodies. [2]

It’s not just widespread natural disasters that pose a threat. Smaller-scale man-made incidents, whether unintentional or intentional, such as terror threats, can also have a significant impact on business continuity. In the aftermath of the Paris terror attack in November 2015, Brussels was put on a heightened state of alert and local officials recommended a full lock down, with several facilities across the city ordered to close. [3]

Heightened state of alert

When a cable fire blazed for 36 hours under the pavement in London’s Kingsway in April 2015, several businesses lost electric, gas and broadband services. Some 5,000 employees were forced to evacuate their offices, with more than half of them experiencing disruption for several days. The estimated cost to London’s economy was £40m. [4] Under this heightened state of alert across the globe, companies must be prepared to relocate their staff at a moment’s notice due to a terror alert or even attack.

Recent flooding in northern Britain during the Christmas period highlighted the vulnerability of businesses to local weather events. More than two-thirds of businesses have been affected by flooding, drought or snow since 2011, and 3200 commercial properties flooded during the wet winter of 2013. But despite this, a study by the Federation of Small Businesses in January 2015 found that 59 per cent of the small businesses that they questioned did not have a plan in place to deal with extreme weather such as flooding or snowstorms. [5]

Prior to the 1980s, if you lost your place of work you would simply take a few days off. Businesses were vulnerable to disruptive events that were out of their control, with lost revenue, diminished reputations, and even the threat of closure. But, during the past 30 years, companies have realised the value of having a disaster recovery plan that includes fully equipped alternative premises to work from. Unlike the 1980s, customers today expect an uninterrupted service even during a disaster, whatever the size of the business – and now there is an expectation to have an effective plan in place. But, astonishingly, despite significant changes to working practices and mobile technology during the past 30 years, recovery methods have largely remained static, and the plight of workers has remained largely ignored.

Shareholder value

The case for Business Continuity was well made by the seminal research by Knight and Pretty “The Impact of Catastrophes on Shareholder Value” first published in 2002 and updated ever since. This showed that shareholder value was lost in the long-term by the poor response to a catastrophe, but conversely it was actually improved by responding well. An

oft-quoted statistic is that 80 per cent of businesses affected by a major incident either never re-open or close within 18 months. Although the empirical evidence for this is elusive, this and similar statistics have been quoted by IBM, Axa, Chubb, FEMA, the ITAA, and other sources.

With natural disasters impossible to predict and an increased risk from terror attacks playing a major role, the need to have an established workplace recovery plan is greater than ever. But today, it is not just your IT systems that need to be recovered. Your most important assets – your employees – must also be prioritised. As connectivity and co-working solutions continue to rise there is a growing expectation that it is business as usual. There are no more excuses, no matter what the disruption.

(1) https://www.americanexpress.com/us/small-business/openforum/articles/hurricane-sandys-impact-on-small-businesses/
(2) http://www.chusho.meti.go.jp/pamflet/hakusyo/h23/h23_1/2011hakusho_eng.pdf
(3) http://www.theguardian.com/world/2015/nov/21/brussels-locked-down-after-terror-threat-level-raised-to-maximum
(4) http://www.standard.co.uk/news/london/holborn-fire-costs-london-firms-40m-full-scale-of-damage-and-disruption-revealed-10150993.html
(5) http://www.fsb.org.uk/media-centre/press-releases/fsb-warning-as-more-than-half-of-small-firms-without-flood-plan-pr-2014-43

The recovery site dinosaur.

Traditional Workplace recovery takes no account of employees' emotions or their journey to work. It is designed for an era when both IT and people were more static.

Most businesses are confident they can recover IT (74 per cent), despite the rising number of technical failures reported by traditional recovery providers. Our research revealed that about one in three of IT recoveries are fully successful, but 1 in 16 completely fails.

However, this focus on IT has come at the expense of people. Modern workforces are increasingly mobile – the practice of herding workers into a 'one-size-fits-all' facility is outdated. Traditional workplace recovery takes no account of employees' emotions or their physical location. In a widespread disaster residential properties can also be affected and workers' concerns will also be directed towards their families and friends.

During a time when travel disruption can be at its worst, it makes no sense to force staff on a long journey to work, at a time when they will resent spending hours on the road en route to a static site that may be difficult to access. It is no longer acceptable for businesses to ignore the needs of their employees, and staff are demanding more from their employers. In order to retain the services of the best workers and stay ahead of their competition, companies are increasingly being forced to look to solutions that allow people to remain closer to home if disaster strikes, allowing them to prioritise their family needs while also putting their work requirements on an even keel.

Case study

When Superstorm Sandy struck, Erin Visalli was one of the thousands of small-business owners whose life was turned upside down. Her store in Ocean City, suffered about $20,000 in losses. She was also forced to evacuate her home with her husband and their one-month-old son. For the next two months, they lived with her parents and in-laws while at the same time trying to get her business back on track. [7]

Smaller firms

For larger businesses, the decision to protect against continuity issues is relatively simple. They will have access to experts in order to make informed decisions of the potential damage and associated costs. But for smaller firms, it can be difficult to research the options fully, and decisions are more ad hoc. However a decision is reached, it is clear that any recovery process that fails to take the needs of employees into account is no longer sustainable.

As a result, many companies are unsurprisingly moving more towards using home working in case of a crisis.

Recovery in numbers

9%

of service providers have never demonstrated their ability to recover in any way.

40%

of businesses rely solely on what their service provider tells them or what is in the contract.

19%

of service providers share testing results with their clients.

31%

of service providers only have successfully recovered from real disruption.

This is more an indication of the failure of traditional disaster recovery plans, as opposed to recognition that working from home is a valid recovery solution.

IDC: "Perhaps the most overlooked aspect of DR planning is the personnel plan. Organisations assume that IT staff will be available to travel to the DR site to manage the failover and new systems. There are two problems with this assumption. First, in the event of a regional disaster, the employee's home, family, and community may be directly affected; the employee may be occupied with personal recovery and not available for IT recovery. Second, as learned after 9/11, transportation systems may be shut down, making travel to the DR centre difficult or impossible." (8)

ISF: "Responsibility for business continuity is often allocated to support functions (such as IT or information security), instead of the business. This allocation can result in business areas believing that business continuity is an IT or information security issue rather than a business issue." (9)

(6) Forrester cesearch: A commissioned study conducted by Forrester Consulting on behalf of IBM, 2013. The Risks of "Do It Yourself" Disaster Recovery.
(7) http://www.entrepreneur.com/article/226520
(8) IDC 2015: Disaster Recovery Planning: Things You May Have Overlooked.
(9) ISF 2015: Aligning business continuity and information security - special project report.

There is a lack of testing of recovery facilities by businesses. This testing would uncover problems that businesses discover only when a disaster strikes, such as:

1 **Too close to the disaster**
If the recovery site is too close to a disaster, then it may be affected by the same incident.

2 **Too small**
If you have bought 'syndicated' seats which are available on a first-come first-served basis, you may find that all available seats have already been taken.

3 **Too far away**
If the recovery site is too far away, workers may be unable to travel long distances leaving families and other commitments.

The widening recovery gap.

Technology continues to change how we work. Traditional recovery solutions have not kept pace.

Mobile working solutions have fundamentally changed the workplace. People can work wherever they sit down, accessing services and data as needed. Cloud computing provides scalable solutions without the need for heavy investment in IT equipment and capabilities, and if disaster strikes, new technology gives us far more options.

But despite companies beginning to embrace new working practices, with an increased reliance on co-working and shared spaces, recovery methods are lagging behind. Gone are the days when we have to stop work or move an entire company, en masse, to a large static recovery location. Today, it is much easier to simply head for the local coffee shop or work from home. But, as we will learn, if not considered properly these solutions bring with them a multitude of additional problems.

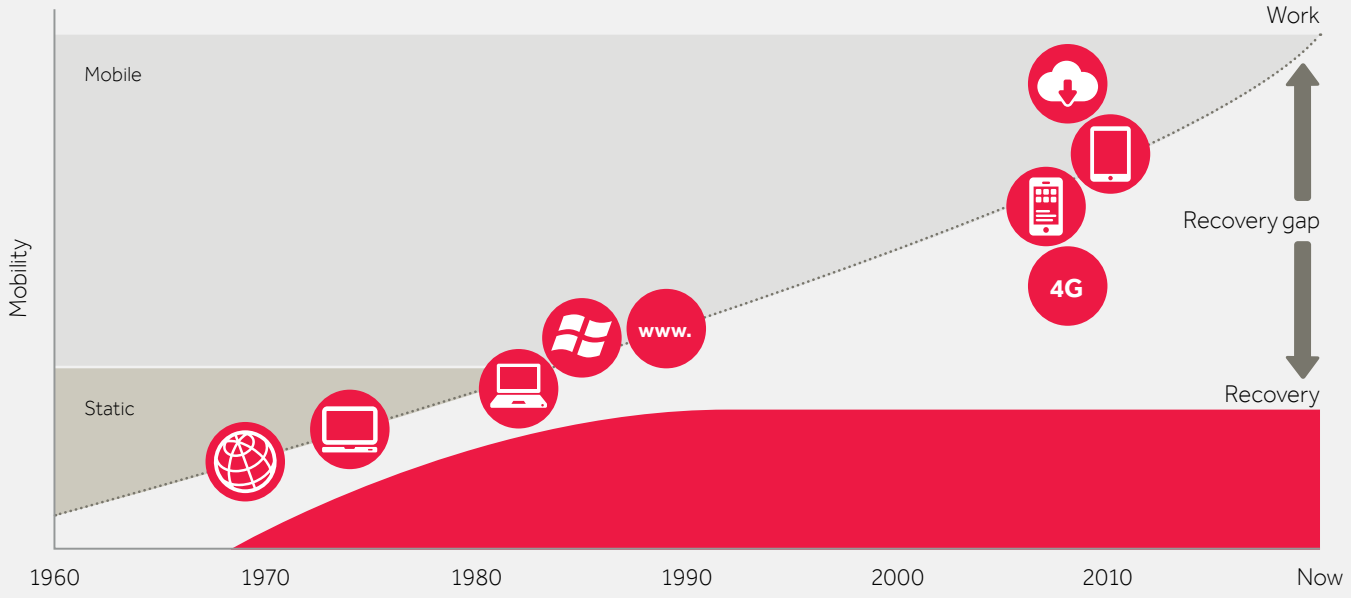
Traditional solutions in decline

With this rise in technology and changing needs of employees, it's not surprising that the popularity of traditional recovery solutions is in decline. But by comparing traditional business continuity plans and mobile solutions it is clear that there is a widening gap between companies' requirements and the recovery options available.

This gap is increasingly being filled by flexible workplace recovery, which utilises a number of flexible office and co-working spaces, offering a real alternative for the future. Regus has seen the demand for their dynamic Workplace recovery solutions double during the past nine months. While some workers may indeed be able to find an ad-hoc solution, this cannot be the complete picture. Vital staff still need to be placed in an office or co-working space that is both convenient and provides a professional working environment. With a combined IT and people- focused approach, businesses can choose from systems that are flexible, fit-for-purpose and regularly tested.

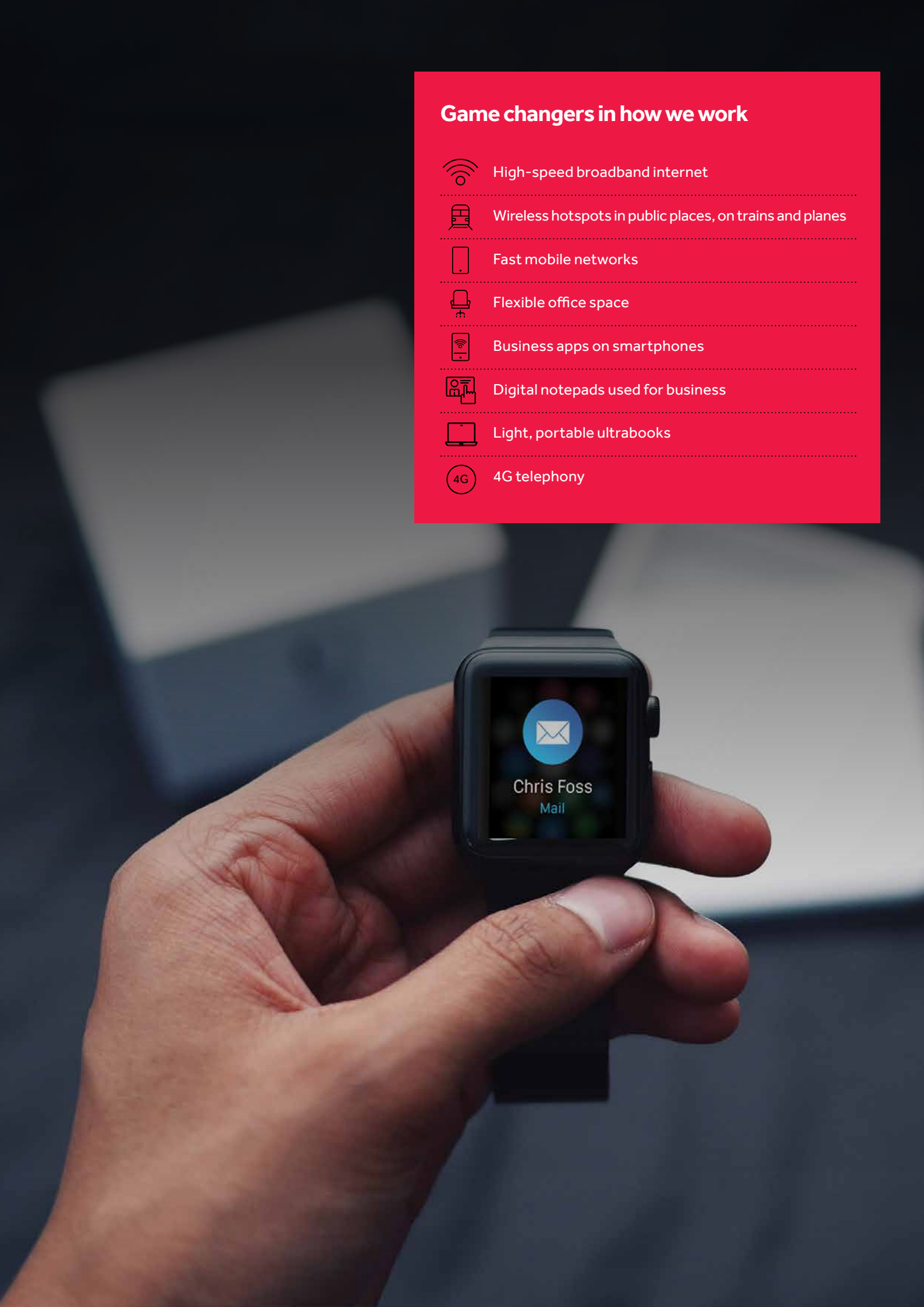
Evolution of the workplace

Despite the advance of mobile technology, recovery methods have not changed since the 1980s, creating a widening 'recovery gap'



Game changers in how we work

- High-speed broadband internet
- Wireless hotspots in public places, on trains and planes
- Fast mobile networks
- Flexible office space
- Business apps on smartphones
- Digital notepads used for business
- Light, portable ultrabooks
- 4G telephony



Is mobile working your panacea?

Businesses are becoming more reliant on staff working from home or in wi-fi enabled locations. But while mobile working offers enormous flexibility – it is inherently resilient and there are few apparent up-front investments or detailed plans needed – it is not without its challenges.

The fastest growing business continuity strategy is to work from home. Our research has shown that this is the preferred option for 39 per cent of businesses, with 75 per cent of these expecting to see an increased reliance on it. When you consider that PwC clients have reported being able to make savings of 50 per cent of their business continuity budget by adopting this strategy, this is hardly a surprising statistic.

Previously, with a lack of professional flexible recovery plans available, working from home has often been the most attractive option for businesses, not to mention the easiest and cheapest to implement. But while this strategy is growing in popularity, unless it is already practiced by employees it is not without risk. The most worrying finding from our survey is that it is usually adopted with very little research into, or testing of, the practicalities or dangers involved.

In addition to security concerns over unsecured wi-fi networks and employees conducting sensitive conversations in public places, the danger of "tiger kidnappings" also need to be taken into consideration. In Dublin in December 2015 a key earner was coerced into helping criminals secure a ransom demand for €200,000, while his whole family was kidnapped and held at gunpoint overnight.

Widespread disasters often present an opportunity for opportunist criminals and fraudsters to exploit. Consider that you are suddenly flooding the streets with employees who are unaccustomed to working remotely on laptops and other mobile devices, then imagine the consequences of just one of these devices being lost or stolen.

IBM (Avoiding the pitfalls of outdated DR plans)

"We'll be able to keep the business running during a disaster because we've developed a work from home strategy" – WFH strategies don't often perform as expected. Employee homes may be damaged during the same disaster that affected the business. Employees who stay at home may not have access to the same information and software as they do in the office, a situation that can have a serious impact on productivity. [10]

Only **14%** of our respondents had looked whether their staff's homes were suitable for home working.

It may be convenient, comfortable and can be activated with the minimum of disruption, but there is a danger of assuming that all workers have an adequate working environment at home.

Case studies

A New Jersey court granted workers compensation survivor benefits to the family of a manager who died of a blood clot after sitting at her work computer at home for long periods of time.

Earlier in the same month, Oregon's Court of Appeals ruled that a woman selling window treatments and bedding was entitled to compensation after she tripped over her dog and suffered a broken wrist while carrying fabric samples from her home to her car. (12)

The home working misconception

The idea of working from home may initially seem like an attractive one, and may indeed be the best option for employees who already practice it, but when used only as an emergency option it makes many assumptions and is rarely sustainable in the longer term.

There is an assumption that all employees have sufficiently fast, reliable and secure internet connections and communication networks. Remember, disasters are not confined to commercial property alone – residential areas can also be hit, and often with far greater consequences. The recent flooding in the north of England should be enough to remind you of the indiscriminate nature of flooding. Relying on an employee living far enough away from the epicentre is akin to having no backup plan. If their home and/or communications are also affected, then you have no other options, and that employee will remain unproductive and out of action.

Consideration must also be given to printers, copiers and any other facilities that are taken for granted. Insurance policies should also be checked and in some cases it may also be necessary to obtain permission from a landlord, where leases may prohibit running a business from home.

Home workers may also be covered by local health and safety legislation, such as the UK's Health and Safety at Work Act 1974, and firms may be obliged to undertake risk assessments and supply suitable equipment such as desks and chairs. Our survey suggests that 80 per cent of businesses have failed to investigate their health & safety obligations for employees working at home, but in every situation it is indisputable that forethought and planning could avoid problems down the line. (11)

(10) IBM 2013: Avoiding the pitfalls of outdated disaster recovery plans
(11) Law at work 2011: https://www.lawatwork.co.uk/commentaries/working-from-home-do-your-homework Working from home? Do your homework
(12) ISF 2010 - part of 'Protecting information in the end user environment': Understanding the security challenges associated with the end user environment.

Working at home may seem like the perfect scenario, but it can cause problems. With people relying on team dynamics and support networks to boost their productivity, the longer a disruption continues, the more isolation becomes an issue.

Keep it together – why working in teams is key to survival

The idea of working at home, especially during a work disruption, can initially seem easy to implement. It may well be the best solution on offer, but it is no panacea. Most businesses understand this, but the lack of viable options leaves them with little choice. Our research revealed that the loss of working in a team was considered to be the least important factor in considering alternative places, but this can be short-term thinking.

Clearing the kitchen table on a daily basis to set up your office may seem easy, but family situations are often not conducive to a productive working environment. It may work for a day or so, but in a widespread disruption it quickly piles additional pressures on an already difficult situation. Without an existing working pattern in place, companies cannot assume that employees have the additional space to easily slot in a workstation, and many may be forced to carve out space for a temporary work station at home, often while attempting to ignore distraction from other family members and children.

And for those workers who do not have the issue of family distractions, the opposite problem often surfaces. Staff working at home can quickly feel isolated, with a lack of interaction with colleagues and managers complicating simple day-to-day tasks. Research reported in the Quarterly Journal of Economics [13] entitled "Does Homeworking Work" listed the following worrying factors for employees not in the office:

- Loss of sense of team
- Isolation of staff as individuals and as professionals
- Lack of support network
- Being out of sight means being out of mind

It is also worth noting that a number of businesses which in the past have encouraged day-to-day home working have reverted to bringing people back to the office – Google, Microsoft, and HP are three high-profile examples.

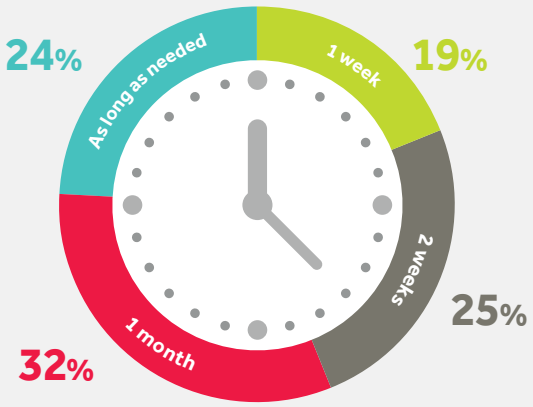
Of course, in a recovery situation workers are not usually forced to work from home for long enough to develop problems related to isolation. But if a workspace is out of action for longer periods, then a backup plan is needed. Bringing employees back together in a temporary office or co-working space, even if only the most vital staff are prioritised reduces the risk and impact of these work from home challenges.

Almost three-quarters

73%

of businesses shared our concern about security. From this, we can reason that security is one of the biggest factors in selecting alternative office locations, so it comes as a surprise to discover that only 25% of the businesses in our research have assessed the security risk associated with working from home.

Working from home, how long is this viable?



Telling Statistics
Iron Mountain, August 2013

18%

of firms offer up any guidance to employees on what sort of paperwork or electronic data is permitted to leave the office environment.

50%

of firms allow employees to use their personal email accounts to send and receive work correspondence.

29%

of home-workers said they had left business documents lying around their house.

19%

of homeworkers say that they had thrown company paperwork in their household bin.

With cyber-crime continuing to rise, working away from the office presents a significant security risk that must be taken seriously. And it is not just wi-fi networks found in cafés, on trains and other public places that are insecure – don't forget prying eyes and ears. If you don't train your staff in how to minimise the risk, you may face some unintended consequences.

Cafés are for hot coffee, not for hot desking

Controlling remote access can provide opportunities for criminals because it is impossible to police who has sight of confidential information. Not only is this a breach of good security practice, it may also contravene data protection legislation, industry regulations and governance requirements, not to mention customer contracts.

It is imperative that staff follow best practices when working away from the office. This means that if home working is part of a recovery strategy, then guidelines for working remotely should be prepared, with training sessions to complement them. When you consider the ongoing media coverage about classified emails sent to and from Hillary Clinton's personal email account, the risks become clearer. [14]

None of this is unique to disaster recovery – the difference is that in a recovery situation reliance on employees working remotely will mean that there will be a higher proportion of your staff that is not properly trained. Your own checks and controls will be under greater pressure, leaving you much more vulnerable to security and data breaches.

Unfortunately, when a company is having difficulties it can find itself more in the public eye, and can attract additional unwanted attention. And although we may prefer to believe that the idea of being threatened to allow unauthorised access or to share confidential information belongs in a Hollywood script, fiction has a basis in reality. [15]

(13) Quarterly Journal of Economics (Bloom et al., 2014): Does working from home Work?
(14) Politico article 2015: http://www.politico.com/story/2015/11/hillary-clinton-email-fbi-probe-215630; FBI steps up interviews in Hillary Clinton email probe.
(15) Iron Mountain, 2013: Press Release: most firms ignore the information security risks of home working

Balancing employee concerns with IT enhances chance of recovery.

Businesses need to strike a balance between the old-style recovery and full-on mobile working. That balance should take the form of a toolkit of strategies that allows them to pick the right mix of approaches for different types of needs. Most importantly, it should to address the needs of people, and not just IT and business functions.

In highlighting the various issues with different recovery strategies, there is no suggestion that any of these approaches is invalid. For example, traditional workplace recovery centres may still have a role to play for some organisations, especially where dedicated fully equipped workstations are a necessity, such as trading operations. Businesses that come unstuck are the ones which don't know what their priorities are, and haven't any real idea about what options they have.

Future recovery plans need to focus on the services that clients need most. How your customers feel about your business is often defined by how you cope in a crisis, and companies that can see disasters as an opportunity to provide a special level of service can emerge stronger.

It is clear that there is an irreversible trend in technology to support "anywhere, anytime" working, regardless of the drawbacks. But the temptation to simply use a default option that relies on a mobile working strategy without proper consideration of the consequences is foolish, and opens up businesses to a host of other potential pitfalls and complaints. While for some office workers, the 'work at home' recovery option will continue to be an option, real issues exist in terms of security and control. Even when proper assessment and analysis, is made, it should become obvious that it is often unsustainable in the long term.

> **"The best prepared businesses have a number of different approaches. They know what matters and what is needed to keep doing it.**

As a much-needed alternative, dynamic workplace recovery offers a flexible 21st-century solution that is compatible with the requirements of workers, companies and their clients. These dynamic recovery solutions allow companies to recover securely, where it best suits them, based upon the event. The ability to activate solutions at short notice in multiple locations is an invaluable tool for business continuity.

These new, dynamic recovery solutions allow companies to recover their employees near where they work, near where they live, or far enough away from a widespread disaster. This approach greatly reduces the reliance upon the capabilities of a single facility or small set of facilities. Instead, resiliency and flexibility is derived from the large network of facilities.

No one solution provides a complete one-stop answer. The best prepared businesses have a number of different approaches. They know what matters and what is needed to keep doing it. They have also paid attention to the needs of employees during a disaster recovery operation. These needs might include:

- Family commitments
- The desire to work within a team
- Access to support networks
- Secure communications
- Modern facilities

Case study

It is easy to find case studies for where businesses get it wrong, but this is an example where good preparation helped a global bank get it right.

From Monday 29th – Tuesday 30th Oct 2012 Hurricane Sandy hit the east coast of the US, resulting in widespread power outages and the closure of main transportation routes across New York, Connecticut, and New Jersey. Many businesses were badly affected.

The bank had invested in resilience and business continuity strategies, including workplace recovery, transference of business and homeworking. Hurricane Sandy put these to the test and the bank was able to cope with minimal disruption having taken the following steps:

A decision was taken before Sandy hit land. The workplace plans were activated.

Resilience measures for the building ensured that the majority of the firm's sites retained power.

Critical staff worked from their work recovery sites, non-impacted buildings and homes.

Global hubs were leveraged to transfer work out of the affected region.

The things that really helped were:

Proactive use of contingency measures and communications to all staff allowed critical operations to be continued.

Resilient buildings allowed primary office and recovery sites to remain operational.

The business did not rely on a sole recovery strategy.

What makes a plan?

Dealing with a disaster well wins the loyalty of your customers. Dealing with it badly can put you out of business.

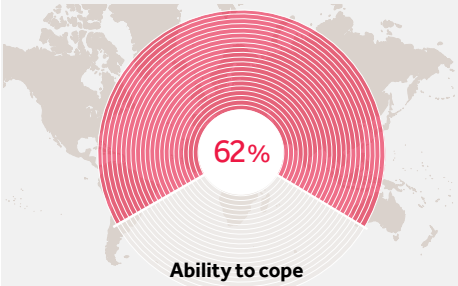
Hoping you can sort things out if they go wrong is foolish. Most businesses instinctively understand this – 74 per cent of the respondents to our survey have a disaster recovery plan, with IT recovery plans far more prevalent. But companies often say that they are not worried about the need for office space after a disaster. The typical attitude is that: "We'll sort it out if the need arises. If necessary, we'll send people to a local Regus office or co-working space."

The obvious fallacy with this statement is that businesses are often not alone in dealing with a disaster, and any spare capacity may already be taken. When you consider the financial risks involved, and the importance placed in keeping clients and staff happy, it is nonsensical and complacent to not consider all of your options and eventualities. And when you consider that, according to research by Aberdeen Group [18] the average cost for one hour of downtime is $8,000 for SMEs, and $700,000 for larger corporates, no matter what size your business it is clear that only the foolish will be out of action for longer than absolutely necessary.

This complacency is exposed when a major area disaster strikes, such as Superstorm Sandy or the Fukushima nuclear disaster following a devastating earthquake and tsunami, or even smaller scale, the Christmas floods in the UK in 2013 and 2015. In all of these situations, widespread power and communications failures meant that many plans which relied on home-working failed. Even the US Federal Reserve was sufficiently disturbed to pass comment:

Survey results

Disaster impact area



Ability to cope in an impact area

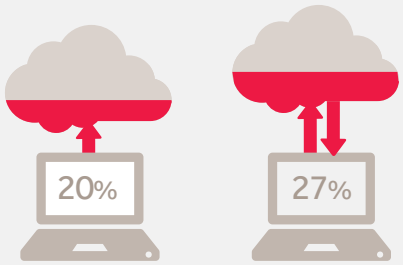
Most businesses (74%) are quite confident in their plans, or at least their ability to cope, even in a disaster impacting a wide area (62%). But this confidence may be misplaced in many cases, with 47% testing their plans once a year or less, and one third of respondents having never tested their ability to work anywhere else.

Actual data recovery

Only 31% recovered their data as planned

Real-life experience is patchy. While 30% have never used their plans, 21% invoke their options most years, or sometimes more frequently. Where they have had to use their plans, 21% say it all worked well. The flip side to this is that it clearly didn't work well for quite a few people. Only 31% recovered their data as planned (most of whom actually lost data), and 23% only had access to systems in line with their plans.

Cloud usage



Reliance of Cloud usage

Reliance on backup and recovery

The reliance of cloud computing is also on the rise – 20% of businesses report that they are using the cloud for business applications, and 27% need the cloud for some degree of back-up and recovery service.

“Business interruption insurance is not an answer to a disaster – it may help limit financial loss, but it cannot return service to the customer, nor restore a lost reputation.

“Firms should be encouraged to revisit their work from home strategies in light of power, telecom and transit problems that were experienced. Firms may be limited in their ability to conduct business if they rely too heavily/solely on this model.” [16]

Another fallacy is to assume that just because you have outsourced your IT recovery solution to a third party, their deeper resources and professionalism will make sure that you will recover safely. In particular, cloud recovery services are still relatively young and their recovery capabilities may not provide the same reliability as the best in-house set-ups.

This will be improved with time, but the risk to your business, and passing the management of that risk to someone else, who may not share your priorities, doesn't change that. Coupled with an increased reliance on the cloud is an expectation that workers can work remotely, especially if disaster strikes. This is often the most obvious solution, but fails to take people into consideration during what is already likely to be a stressful time for all involved.

Equally, business interruption insurance is not an answer to a disaster – it may help limit financial loss, but it cannot return service to the customer, nor restore a lost reputation.

Your business is most vulnerable when an unpredictable disaster strikes. Without a proper plan that considers every available solution, the chance of failure is greatly increased. But get your employees' needs right and your clients will see that you are putting their interests first, even in difficult times. Get it wrong, and you could find yourself out of business.

With this in mind, the best plans will strike a balance between

- Dedicated workplace recovery for critical staff needing specialist equipment.
- Pre-designated office space for staff dealing with confidential information.
- Non-critical staff working at home during a recovery period
- Facilitated flexible office spaces to maintain a team approach and allow access to facilities.

Policies will be adapted to allow for remote working and training to help people work safely and securely, even in cafes, on trains and other public areas.

Whichever combination of solutions is used, the plight of your staff must be considered at every stage, and for every eventuality. Clients will no longer accept excuses for anything less than the minimum of disruption. If your employees cannot function properly, then at least be prepared to consider the consequences.

Datamonitor Financial's 2014 SME Insurance Survey

Small businesses in the UK feel most at risk from an event that would disrupt their ability to trade.

28% were very concerned about the potential for a natural disaster such as flooding to leave the business unable to trade.

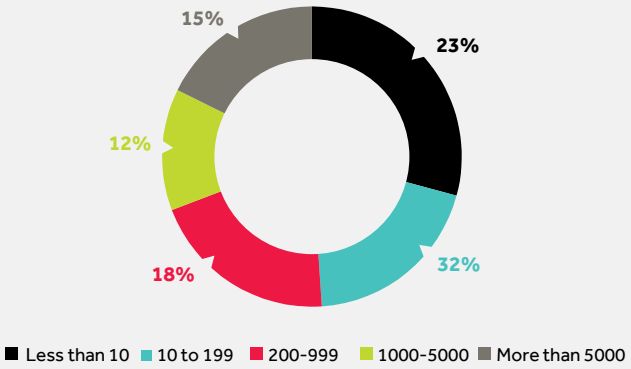
However, despite these concerns, fewer than one in four of SMEs surveyed have a business interruption insurance policy. [17]

(16) PwC Business Continuity Blog 2015: US Federal Reserve statement (To confirm)
(17) Datamonitor Financial 2014: SME Insurance Survey
(18) http://www.aberdeen.com/research/8623/ai-downtime-disaster-recovery/content.aspx

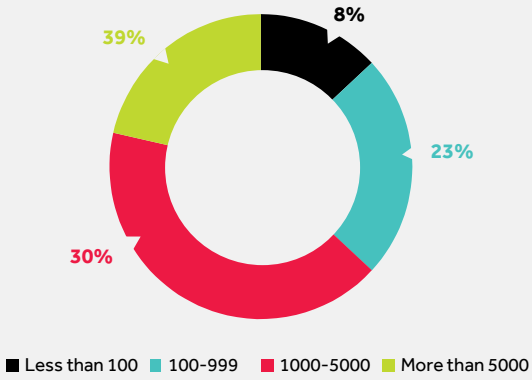
Our research.

Our research was conducted in November-December 2015, and took the form of two questionnaires. The first was specifically targeted at Business Continuity professionals ('Experts'), which drew 212 responses. The second was targeted at business users of office space services ('Business'), and this drew 2653 responses.

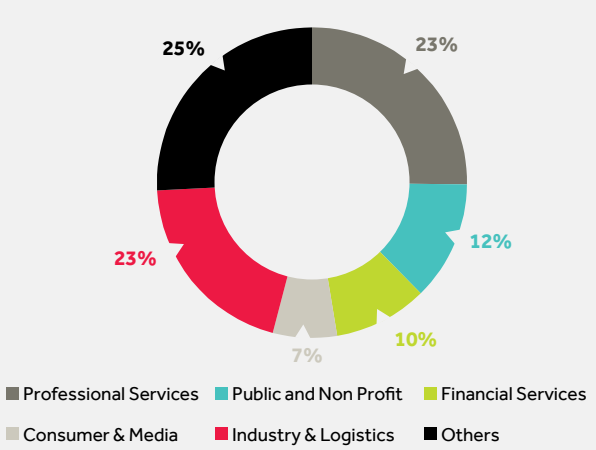
Business Responses - Size of organisation



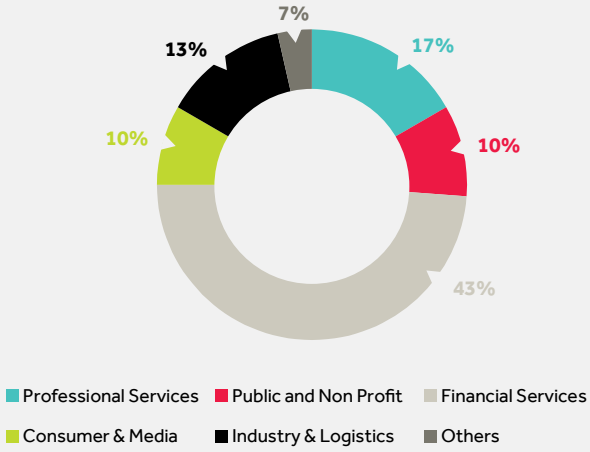
Expert Responses - Size of organisation



Business respondents by industry



Expert respondents by industry



Checklist.

It's easy to assume people can work away from their current office. But there are many other factors to consider: how long can they do it for? How secure is it? Is there capacity for high volumes of people, data and hardware? This checklist will help you assess how much support you need.

Choosing the right location

1. Proximity to current locations	Are there good transport links for staff and visitors?
	Is there sufficient parking for staff and visitors?
	During certain incidents such as a power cuts and evacuations, is the location far enough away from the existing office to not be impacted by the same event?
2. Size, capacity and availability	Are there enough seats, desks and offices at the single location or will you need to agree additional space elsewhere?
	How readily available will the office be for your staff and visitors?
	Have other companies also contracted with the site to accommodate them during an incident of their own? – you may need to invoke at the same time, reducing the space for your organisation.
3. Budget	Have you confirmed your budget for additional space?
	Confirm the cost per capita, desk and room over time.
	Confirm the costs for use of equipment.
4. Dedicated vs. syndicated seating	Do you need dedicated seating for year round access (more expensive) or syndicated seating for first come first served access – competitors or local organisations may also have a contract (less expensive)?
5. Physical and Non-physical security	How safe are the premises and what security measures are being taken to protect staff and information?
6. Mailing facilities	Will you be able to effectively redirect post to the new location?
7. Reliability during an incident	Will the location be willing to run exercises with you to validate recovery assumptions such as recovery time, equipment, access etc.

Staff requirements

1. Team motivations	Will staff be happy and motivated to work from the new location?
	Do your staff need to be together or can they work remotely elsewhere?
	Is the new location as accessible for staff and will they be happy to travel there?
2. Staff reimbursements	How will staff be reimbursed for additional costs incurred through additional travel, sustenance, parking, child care, longer hours etc.
	Will there be a specific expense policy for relocated staff?
3. Staff security	Is there appropriate support for staff on site at all times?
4. Staff working from home	Does your organisation need to do a home risk assessment and security check?
	Will you create a working from home policy?
	Do they have the minimum IT (software, hardware, capacity and connectivity) requirements to complete their roles?
	How will they be reimbursed for any additional expenses?
	Will they be provided with home support and equipment?

Confirming your numbers

1. Space and seat number requirements	Have you confirmed your critical and priority departments and activities to recover?
	Do you know which ones you need to prioritise over a period of time?
	Confirm the roles and number of people needed to perform these activities over different periods of time.
	How many could work from an alternate location (e.g. home)?
2. Requirements over time	Critical time periods may impact your numbers and priorities at different times e.g. recurring deadlines, end of month activities, reporting etc. – consider how your needs will change depending on when the incident may happen.
3. Dependent activities and departments	In larger organisations, many departments and activities may be interlinked and dependent on each other – consider how this affects the numbers of people needed along the process flow.
4. Senior leadership and/or crisis management teams	Is there an additional requirement for rooms dedicated to senior leadership or crisis management teams throughout the incident?

Technology requirements

1. IT systems	Which systems are needed to support the activities and people?
	How quickly do the systems need to be recovered to support the activities and people?
	Can you get access to the recovery site quickly enough to meet this need?
	Who will be responsible for the set up and installations?
2. Hardware	Which hardware is required for the activities and staff?
	How quickly can the hardware be provided or sourced upon invocation to meet your recovery needs?
	Are there 24/7 power generators to support equipment and staff?
3. Telecommunications	Who are the providers, can that be negotiated and what are the associated costs?
	Confirm the internet connectivity, speed and capacity for your activities.
	How will you redirect phone lines and numbers?

Regulatory requirements (for larger organisations)

1. IT systems	How will the location meet your regulatory obligations?
	• Information security
	• Physical security
	• Speed of recovery for customer focussed activities
	• Privacy
	• Storage, archiving and data sensitivity
	• Health and Safety at Work.