

Business resilience

Ensuring continuity in a volatile environment

A report from the Economist Intelligence Unit
Sponsored by ACE, IBM and KPMG





About the survey

The Economist Intelligence Unit surveyed 181 executives around the world in January 2007 about the challenges and opportunities they face in their efforts to increase business resilience. The survey was sponsored by ACE, IBM and KPMG.

Respondents represent a wide range of industries and regions, with roughly one-third each from Asia and Australasia, North America and Western Europe. Approximately 65% of respondents represent businesses with annual revenue of more than US\$500m. All respondents have influence over, or responsibility for, strategic decisions on risk management at their companies.

Our editorial team conducted the survey and wrote the paper. The findings expressed in this summary do not necessarily reflect the views of the sponsors. Our thanks are due to the survey respondents for their time and insight.



Business resilience

Ensuring continuity in a volatile environment

Executive summary

The success of a company depends on its ability to identify and manage successfully the risks associated with running its operations. These risks—which can be grouped under the heading operational risk—refer to any type of risk a company faces that is neither financial nor market-related in nature. For example, this category might include risks associated with the supply chain, IT systems or business processes.

In the past few years, business continuity management has emerged as one of the key tools that companies use to manage operational risk. At the same time, the discipline has evolved from being one that is focused on the way in which companies respond to an unforeseen event, to one that is used to increase their preparedness and overall resilience. In this report we look at areas of operations in which executives say they feel most threatened, explore some of the tools that they use to mitigate these risks, and highlight areas of particular strength and weakness in companies' consideration of operational risk management and business continuity.

Key findings from this research include the following:

- **Data are the key concern.** Our survey of 181 risk executives underlines the importance of information technology (IT) to the smooth running of the organisation. When asked what they considered to be the most important threat in their consideration of operational risk management, 36% selected loss of data and 31% selected systems failure. Human error, another key concern for operational risk managers, was cited by 35% of respondents.

- **A day is all it takes.** Just under half of all respondents—47%—said that they could endure less than a day of downtime from their IT systems before the disruption became serious enough to jeopardise

the survival of the entire company. This finding is corroborated by other surveys: according to the US National Archives and Records Administration, 25% of the companies that experienced an IT outage of two to six days went bankrupt immediately.

- **Commitment to a business-wide approach.** There is widespread acknowledgement that operational risk and business continuity issues should not be confined to individual functions or departments. Seventy-six percent of respondents agreed that operational risk should be an issue that involves all business units, and 69% took a similar view about business continuity planning.

- **Strengths and weaknesses of communication.** Respondents are reasonably confident about the processes they use to identify risks and to ensure that the board is made aware of significant problems, with 61% saying that they conduct risk assessment successfully, and 52% giving themselves a similar rating for reporting on key risks to the board. Communication with employees, and with the extended enterprise, tends to be less successful, however. Only 31% of respondents say that they communicate successfully on operational risk issues with employees, and just 19% give themselves a similar rating for their communication with the extended enterprise.

- **Stakeholders pile on the pressure.** Although many companies will doubtless recognise the need for robust business continuity plans for their own benefit, pressure to strengthen planning also comes from a variety of external sources. When questioned about the influence that stakeholders have on decisions about business continuity, 59% cited customers as being a significant source, 58% cited regulators and 50% cited investors.



● **Putting plans into action.** Evidence for the importance of business continuity comes from the variety of incidents that have caused respondents to put their plans into action. A total of 27% said that they had implemented business continuity plans because of power outage, 23% because of an attack from a virus or worm, and 21% as a result of supply chain disruption.

● **Reputation is the biggest concern.** Failure to put in place robust business continuity plans can have a variety of negative impacts, including loss of revenue and decline in shareholder value. But among respondents questioned for this survey, damage to their reputation is seen as the biggest threat, with 43% of respondents saying that this is their greatest concern.

● **Small companies lag behind larger peers.** Respondents from companies with annual revenue of less than US\$500m were much less likely than larger companies to consider themselves successful at specific aspects of operational risk management. For example, just 18% consider themselves to be successful at actively testing business continuity plans, compared with 31% of companies with revenue in excess of US\$1bn.

Introduction

Risk has always been part and parcel of doing business, and every company seeks in some way to prepare for damaging incidents and to respond to them as best it can. But in recent years, the need to demonstrate resilience has been given greater urgency as a result of a number of powerful trends. First, a series of high impact, low probability events has alerted executives to the need for precautions. Beginning with the Y2K scare at the turn of the new millennium, and followed by the devastating September 11th attacks, the 2005 hurricane season in the US and a number of other catastrophes, the vulnerability of business to unforeseen events has never been more evident.

In the same period, the trend in business has been towards greater leanness and efficiency. Companies have stretched their supply chains to the limit, sourcing goods from ever more distant destinations and reducing levels of inventory to a matter of days. They have stripped layers of management in an attempt to streamline their organisations and reduce costs, and they have outsourced non-core business processes to external providers. Finally, they have come to rely so heavily on their IT systems that, even if they suffer just a few hours of downtime, the survival of the entire organisation could be threatened.

This powerful combination of highly visible threats, reduced redundancy and greater reliance on IT has pushed the need for business resilience to the top of the agenda. Business continuity and disaster recovery, which were hitherto seen as dull but necessary adjuncts of doing business, have drawn boardroom attention and intense scrutiny from investors, customers, regulators and other stakeholders. Across industries and regions, executives are asking themselves about the threats they face, and what they should do to prepare for and recover from a wide range of potentially devastating incidents.



Business resilience

Ensuring continuity in a volatile environment

The threat from “business as usual”

Media coverage of the threat from global terrorism and pandemic bird flu has done much to focus the minds of executives on the need to make their organisations more resilient. But while high-impact events of this nature should certainly be considered with great care, they are just the tip of the iceberg in terms of the real risks that companies face. Although lacking the immediate impact of a major catastrophe, a whole range of other, more mundane incidents can be just as damaging to the wellbeing of an organisation. Power outage, data loss, application failure and human error may not grab the headlines, but they can have devastating consequences. According to the US National Archives and Records Administration, 25% of the companies that experienced an IT outage of two to six days went bankrupt immediately. The same study shows that 93% of companies that lost their data centre for ten days or more filed for bankruptcy within a year.

The way in which a company prepares for and responds to an incident—whether major or mundane—can make a dramatic difference to its long-term performance and reputation. In 2000, for example, a minor fire at a semiconductor manufacturing plant in New Mexico operated by Philips, the electronics company, led to very different outcomes for the factory’s two main customers, Scandinavian handset manufacturers Nokia and Ericsson. Philips initially told its customers that the factory would resume production within a week, but it greatly underestimated the scale of the disruption caused by smoke and debris to the sterile environment required for chip production. In the end, it took many months to restore the factory and resume production.

Nokia responded to the fire by immediately sourcing other supplies and putting pressure on Philips to provide alternative sources of chips from

other factories. Ericsson, meanwhile, assumed that the fire was a minor technical glitch and waited for normal business to be resumed. By the time it realised the magnitude of the problem, it was too late. The company was unable to find alternative supplies and production of its new generation of handsets was severely affected. At the end of 2000, Ericsson posted a loss of US\$2.34m, much of which could be attributed to the disruption in chip supplies caused by the New Mexico fire. Nokia, meanwhile, went on to increase its share of the handset market from 27% to 30% in the six months that followed the incident.

The different responses of Nokia and Ericsson to what initially seemed a minor disruption illustrate an important point about the need for businesses to prepare effectively for a wide range of incidents. In order to demonstrate that they are resilient in the face of the full range of threats that they face, companies need much more than a “disaster recovery” plan. Far more important is a clear understanding of the threats the company faces, its vulnerabilities and weak spots, and the steps required to formulate a quick and effective response.

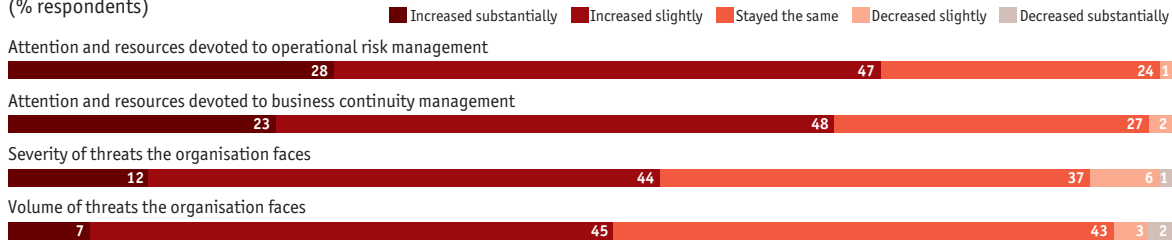
Perceptions of risk and threat

It is often said that the world is becoming a riskier place, but among the 181 executives questioned for this report, there are contrasting views as to whether this is the case. Just over half of respondents, 56%, think that the severity of threats they face has increased over the past three years, while 52% think that the volume of threats has increased. This leaves a sizable minority who think that the volume and severity of threats has either stayed the same or declined.

Respondents may disagree about whether the nature and extent of threats have changed, but there is little doubt that recent years have seen a substantial increase in the attention devoted to preparing for



In the past three years, what change has there been to the number and severity of threats that the organisation faces, and what change has there been to the attention and resources devoted to operational risk and business continuity management?
(% respondents)



Source: Economist Intelligence Unit survey.

them. Of the respondents to our survey, 75% say that they have increased the amount of time and resources they dedicate to operational risk management and 71% have increased the time and resources they devote to business continuity.

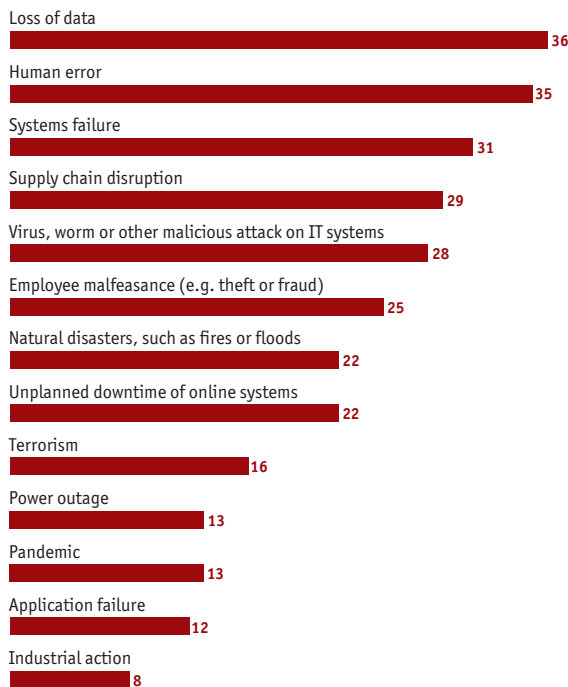
In terms of the threats they face, respondents point to a wide range of concerns ranging from the spectacular to the mundane. Loss of data and human

error are the most feared threats, with 36% and 35% respectively citing these two considerations as among their biggest worries. More catastrophic events, such as natural disasters, terrorism and pandemics, come further down the priority list, with 22%, 16% and 13% respectively seeing these incidents as important concerns.

Given the current focus on bird flu and the concerns being expressed by governments and regulators, it is perhaps surprising that the threat from pandemic is seen as such a low priority. Broadly speaking however, the order of priorities expressed by respondents reflects the reality of threats that their organisations face. Companies should of course plan for major catastrophes, but they should also recognise that such events are, thankfully, comparatively rare. It is far more likely that they will need to contend with a power cut or a systems failure caused by human error, and this should be taken into account when companies look at the operational risks they face. Indeed, when asked about events in the past three years that had caused them to invoke their business continuity plans, the most common causes were power outage and unplanned downtime of online systems, both of which were cited by 27% of respondents.

Which of the following types of threats are seen to be most important in your organisation's consideration of operational risk management planning?

(% respondents)



Source: Economist Intelligence Unit survey.



Business resilience

Ensuring continuity in a volatile environment

External drivers for greater resilience

Beyond any perception that the world may be becoming a more dangerous place, there are several sources of external influence that are encouraging an increased focus on operational risk and business continuity. According to respondents questioned for this report, customers are the stakeholder that is seen as most important in driving decisions about business continuity, with 59% citing them as a significant influence.

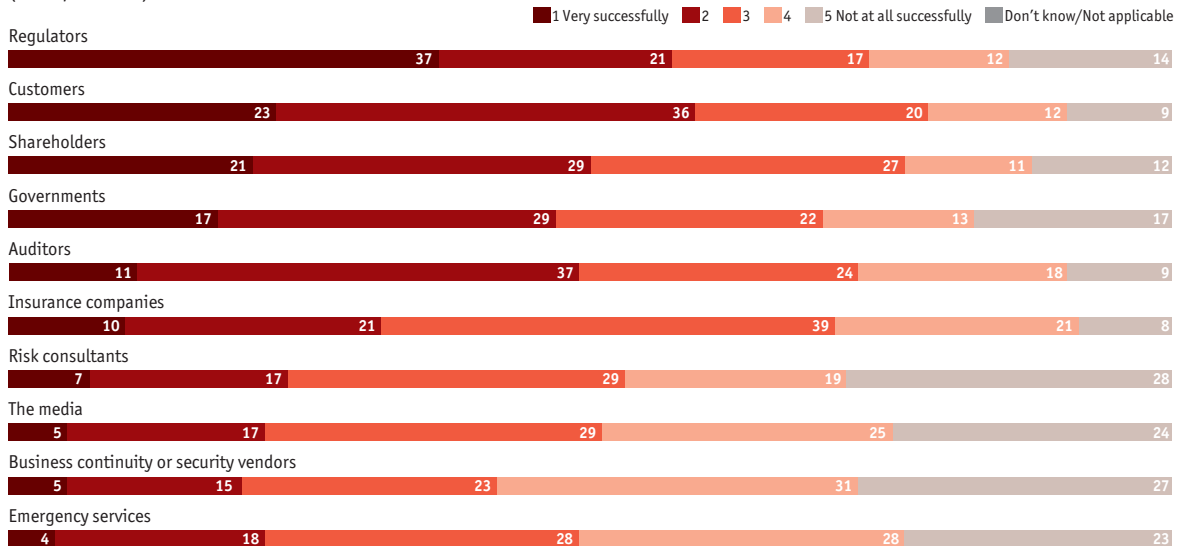
As they take steps to increase the efficiency of their supply chain, companies have become dependent on a highly complex network of suppliers and partners. Over time, they have also consolidated their supplier base, so that they are more reliant than ever on the ability of those companies to deliver on their promises. As a result, those responsible for sourcing decisions are increasing the rigour with which they question suppliers about their level of preparedness.

In the past, organisations tended to ask their suppliers only very basic questions about business continuity but, in the past couple of years, the approach has become more sophisticated. Rather than simply asking whether the supplier has a business continuity plan in place, customers will now ask about the scope of the plan and request evidence of compliance with particular policies.

In addition to customers, pressure from regulators is also becoming more pronounced. Recent regulatory activity, including the Sarbanes-Oxley Act in the US, and the Basel II accord for financial services companies, has focused attention on the need for robust risk management, especially in the area of information technology. Among respondents questioned for this report, regulators are seen as the second most important external influence over decisions about business continuity, with 58% seeing them as significant in that regard. This figure rises to 72% when we consider only respondents from financial services companies.

Simon Mingay, a research vice-president at

How significant is the influence that the following external organisations have over your decisions about business continuity planning?
Rate on a scale of 1 to 5, where 1=Very significant and 5=Not at all significant.
(% respondents)



Source: Economist Intelligence Unit survey.



Gartner, the business analyst, points out that it is not so much the existence of regulation, but the extent to which compliance is enforced, that is the driver for more rigorous business continuity. “You may well find that a regulation spans a geographic region,” he explains, “but in some areas the regulator is either ineffective or is just not doing their job. As a result, lots of organisations largely ignore it.”

Recognising that even minor disruptions can have a dramatic effect on share price and reputation, investors are also starting to scrutinise companies for evidence that they have planned accordingly. As a result, more and more companies are including references to operational risk and business continuity in their annual reports, in an attempt to reassure investors. Among our survey respondents, 50% say that their shareholders exert a significant influence on their business continuity decisions.

Finally, insurers are another important constituent that is encouraging a sharper focus on business continuity, especially in the wake of huge losses such

as the 2005 hurricane season. By demonstrating that they have put in place well-planned measures to deal with any potential disruptions, companies may be able to expect to pay lower premiums. In our survey, 31% of respondents said that the influence wielded by insurance companies over business continuity was significant.

Steps towards resilience

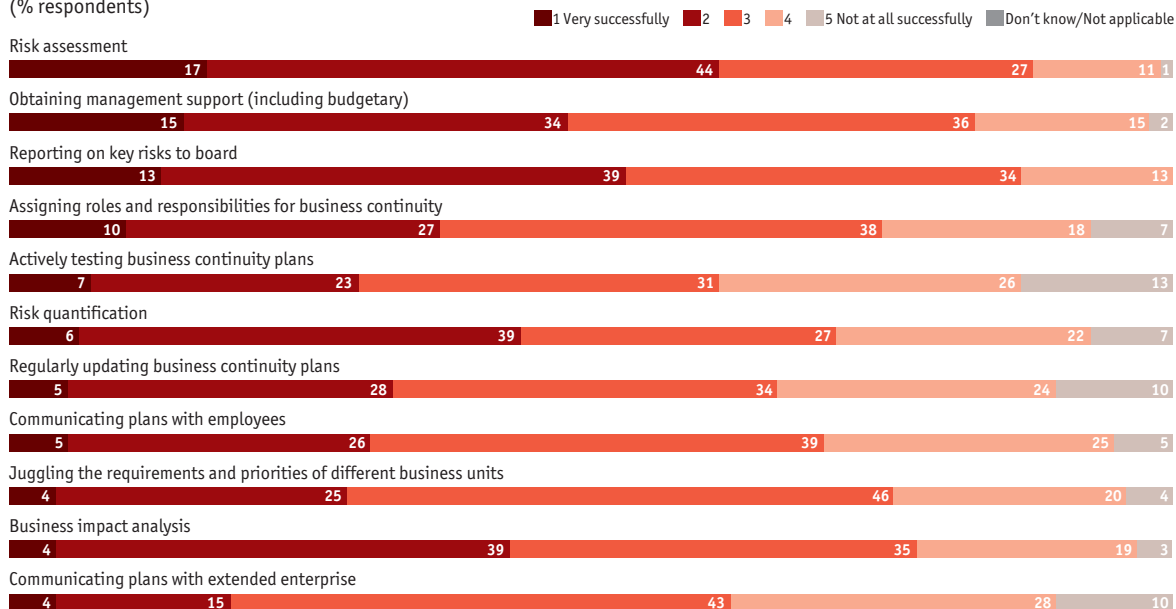
The traditional approach to business continuity involved thinking through the steps that companies should take in response to a major incident, but as Mr Mingay points out, this approach is both outmoded and dangerous. “One of the things that people need to get into their heads is that business continuity is not just about the disaster recovery plan,” he explains. “It’s also about how you do business, where you do business and where work gets done.”

The successful management of operational risk and business continuity requires companies to conduct a thorough assessment of the risks and vulnerabilities

How successfully do you think your organisation manages the following aspects of operational risk?

Rate on a scale of 1 to 5, where 1=Very successfully and 5=Not at all successfully.

(% respondents)



Source: Economist Intelligence Unit survey.



Business resilience

Ensuring continuity in a volatile environment

they face in their day-to-day operations. Among respondents to our survey, there is a relatively high degree of confidence in the ability to assess risks, with 61% considering themselves successful in this area.

“The first question companies need to ask themselves,” explains Charles Skinner, operations manager of Janusian Security, a subsidiary of the Risk Advisory Group, “is what is it that they do and what is mission critical to their company. Once they have understood this, they can then understand the critical processes and deliverables that they have to guard against from an unexpected event.”

Some risks will be common to all businesses—for example, the need to prepare for possible pandemic flu outbreak or power outage—but others will be specific to the company’s industry or location. Careful risk and vulnerability assessment, perhaps using tools such as scenario planning, can focus the minds of executives on the level of the threat that they face and help them to decide where resources should be allocated and where priorities should be set.

Having determined what the risks are, companies then need to get to grips with the likelihood of those risks. Here, respondents to the survey demonstrate slightly lower confidence, with 45% rating themselves as successful at risk quantification.

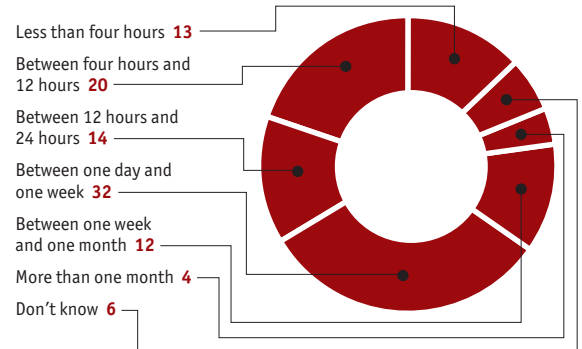
The next step is to assess the effect that a range of incidents would have on the company, using a business impact analysis. This is again an area where slightly less than half of respondents—43%—consider themselves to be successful.

A business impact analysis requires companies to ask themselves what would happen if, for example, a power outage shut down the email server for six hours, or what would happen if a police cordon shut off access to the head office. Is the company more or less vulnerable than its peers to particular disruptions, perhaps because of its location or a quirk of its organisational structure?

This exercise helps companies to assess which services are critical to the running of the business,

How long could your organisation last before downtime of IT systems becomes an issue that could jeopardise the entire company?

(% respondents)



Source: Economist Intelligence Unit survey.

and to think through areas where alternative provisions need to be made. For example, if a company determined that a power outage of any kind is absolutely unacceptable, then that company may want to consider installing an emergency generator.

A disaster recovery plan may be only a small part of ensuring business resilience, but it is nevertheless an essential one. This sets out roles and responsibilities for getting systems and business processes back on track, documents the activities that are required to resume operations and determines acceptable recovery times.

“There are two key parameters that people manage around business continuity management,” explains Mr Mingay of Gartner, “and those are recovery time objective (RTO) and recovery point objective (RPO).” The former, RTO, refers to the maximum amount of time that can be tolerated to resume a particular service or system to full operation, and the latter, RPO, refers to the historical point in time to which the company aims to recover its data.

As companies rely more on their data and IT systems, both RTO and RPO are being squeezed down to a matter of hours. This concern about compressing recovery windows is one that appears to resonate with our survey respondents. When asked how long



they think they could survive the downtime of their IT systems before the problem became one that threatened the survival of the company itself, 47% thought that they would last less than 24 hours.

Managing the plan

Once a company has created a business continuity plan, it is essential that it is tested on a regular basis and updated at least every year in order to reflect changes in the underlying business. Full simulations of particular incidents—possibly in collaboration with partners and customers—can also be a valuable way of testing the resilience of a plan and pointing out weak spots that may need to be addressed as part of ongoing maintenance.

Companies that fail to update their plans are in for a shock should they ever have to use them, says Mr Skinner of Janusian. “Within six months you’ll find that the plan is out of date because of things like staff turnover, a change of business process or a move to a new office,” he explains.

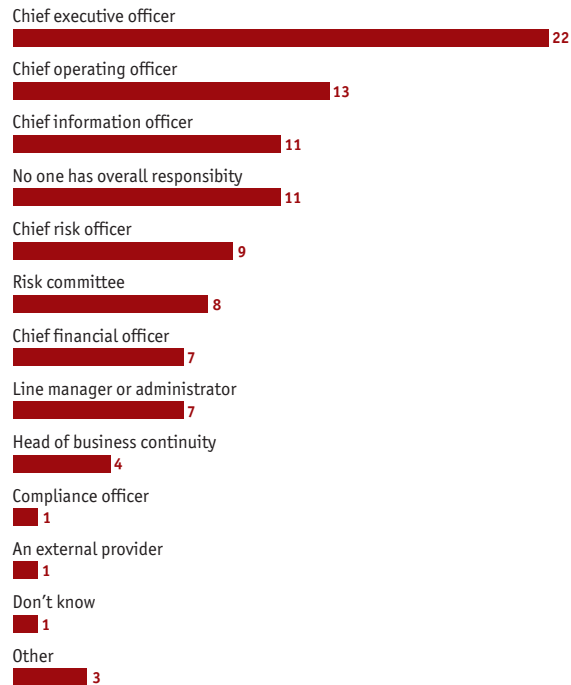
Among respondents questioned for this survey, 58% say that they actively test their business continuity plans at least every year. However, 17% either see business continuity planning as a one-off exercise or do not have a plan at all.

Mr Mingay believes that ineffective business continuity planning is often the fault of poor leadership. “The thing that distinguishes organisations that do this well from those that don’t is leadership,” he explains. “The leadership team needs to show an interest in the process, ask questions, and then put in place the appropriate governance and controls to make sure it happens.”

Another important responsibility for the leadership team is to ensure that sufficient resources are allocated to the consideration of business continuity. “In many companies today, everyone seems to be double-hatted and this causes a huge problem,” explains Mr Skinner. “You look at the day-to-day job of the person who is tasked with business continuity and

Who is primarily responsible for business continuity planning in your organisation?

(% respondents)



Source: Economist Intelligence Unit survey.

you find that it is very difficult for them to set aside the 20% of their time that they really need to manage the plan effectively.”

Because business continuity focuses so much on technology and people issues, there is a danger that it can be seen to be primarily the responsibility of those departments. This is a mistake, says Mr Mingay. “Business continuity is no more or less an IT issue than it is a marketing issue, an operations issue or an anything else issue,” he explains. “The only way you can manage this process effectively is by combining strong leadership with a distributed approach.”

Among respondents questioned for the survey, there is widespread support for the idea that operational risk and business continuity should be business-wide issues driven by board-level executives. Just 27% say that they see business continuity as primarily an issue for the IT and HR departments, and



Business resilience

Ensuring continuity in a volatile environment

just 21% think similarly about operational risk. In addition, 58% say that a C-level executive, such as the chief executive officer, chief financial officer or chief risk officer, has overall responsibility for operational risk in their organisation, while 63% say that business continuity is their responsibility.

This makes sense, especially given that decisions about business continuity planning can have such a dramatic impact on a company's future viability. When asked what they consider to be the biggest threats arising from poor business continuity planning, 43% of respondents selected damage to their reputation. This finding illustrates how customers, the media and other stakeholders will have little sympathy for a lack of robust planning in the face of an incident. It is now expected that companies should make appropriate provisions, and failing to do so will reflect badly on the company's long-term reputation.

Why small is not always better

Although many large companies have made business continuity a priority in recent years, smaller companies have often been slower in their response. In large part, this is to do with knowledge and resources. There is a perception that business continuity solutions, such as risk consultancy, disk mirroring, digital vaulting and remote back-up centres, are only within reach of the deep pockets of the largest corporates. In addition, smaller companies may not have dedicated IT departments or risk managers who are tasked with putting these plans into place. As a result, they generally show much lower levels of preparedness than their larger peers.

Respondents to our survey from companies with annual revenue of less than US\$500m were much less likely to rate themselves highly for aspects of operational risk management. Just 18% considered themselves to be successful at actively testing business continuity plans, and only 20% at regularly

updating those plans. Less than one-third, 31%, say that they use simulations or active testing of their business continuity plans, and just 25% say that they communicate their plans and procedures regularly with employees.

As the costs of storage technology continue to fall, the higher-end technologies are coming within reach of a growing number of businesses, so they should not discount these options altogether. "From a technology point of view, costs have come way down with things like disk storage, which makes that technology more affordable for smaller organisations," says Mr Mingay. "Because of falling costs, small and mid-sized organisations are today using technological solutions to mitigate risk that, two years ago, were only accessible to large organisations."

Moreover, business resilience need not be about costly managed services and technological solutions. "You don't have to spend lots of money," continues Mr Mingay. "It's more about allocating some time and people resources to pay attention to the issue, to think about it and to factor it in as something you should consider. The fact that small companies sometimes don't is less to do with resources and more to do with human nature. We all tend to believe that bad things happen to other people."



Conclusion

The minds of corporate executives have rarely been as focused on the need for business resilience. The threat from major catastrophes, such as a terrorist attack or pandemic disease, has encouraged companies from all sectors and regions to think through their operations and look for areas in which they may be vulnerable. In doing so, they also make themselves more resilient in the face of more mundane (and far more likely) interruptions, such as power outages and human error.

There is widespread recognition among survey respondents that operational risk and business continuity are business-wide issues that require executive board attention. This is good news, as it is only through the engagement of the senior leadership team that the appropriate resources, processes and controls can be put in place.

But although most companies questioned take the issue of business resilience seriously, there are important gaps in their planning and management. A minority of respondents rated themselves as being effective at regularly updating and testing business continuity plans, and only small proportions saw themselves as good at communicating with employees or external partners.

As external stakeholders, including regulators, investors and customers, become more vocal in their calls for greater levels of resilience, there is a pressing need for companies to maintain their focus in this area. The potential for loss that can ensue from failure to protect the company, in terms of damage to assets, lost revenue and tarnished reputation, is simply too great.

Appendix: Survey results

Business resilience

Reducing vulnerability and increasing preparedness

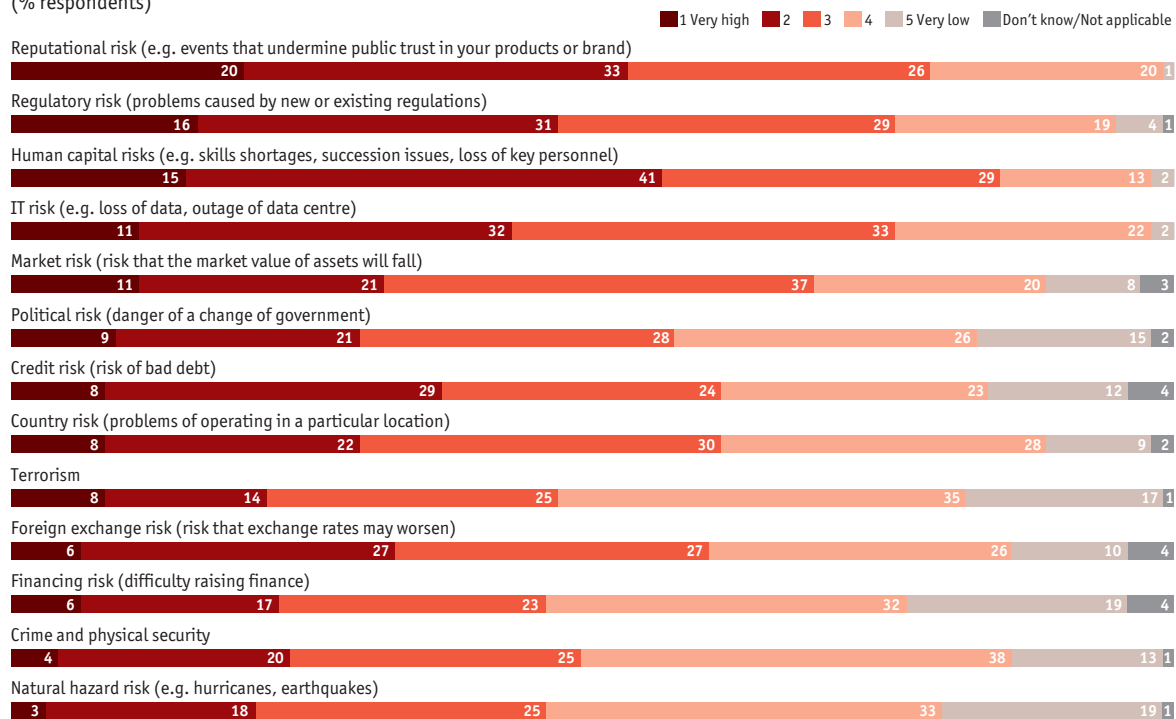
Appendix: Survey results

In January 2007, the Economist Intelligence Unit conducted a survey of 181 executives around the world. Our sincere thanks go to all those who took part in the survey. Please note that not all answers add up to 100%, because of rounding or because respondents were able to provide multiple answers to some questions.

How significant a threat do the following risks pose to your company's global business operation today?

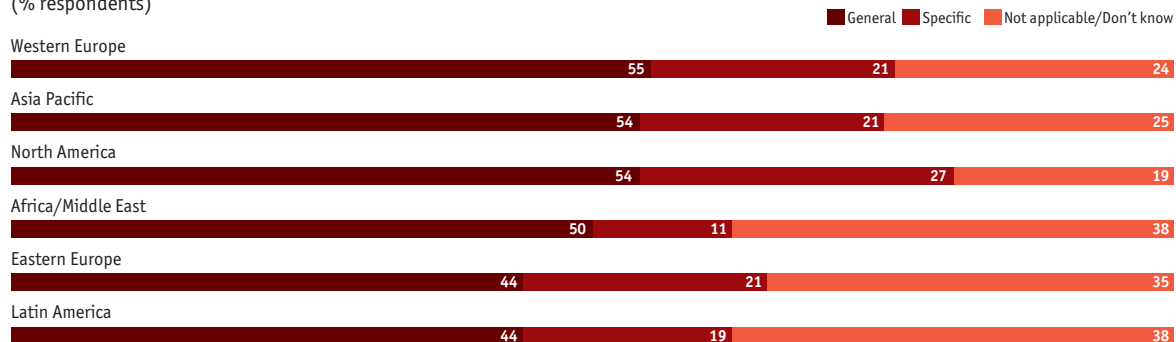
Rate on a scale of 1 to 5, where 1=Very high risk and 5=Very low risk.

(% respondents)

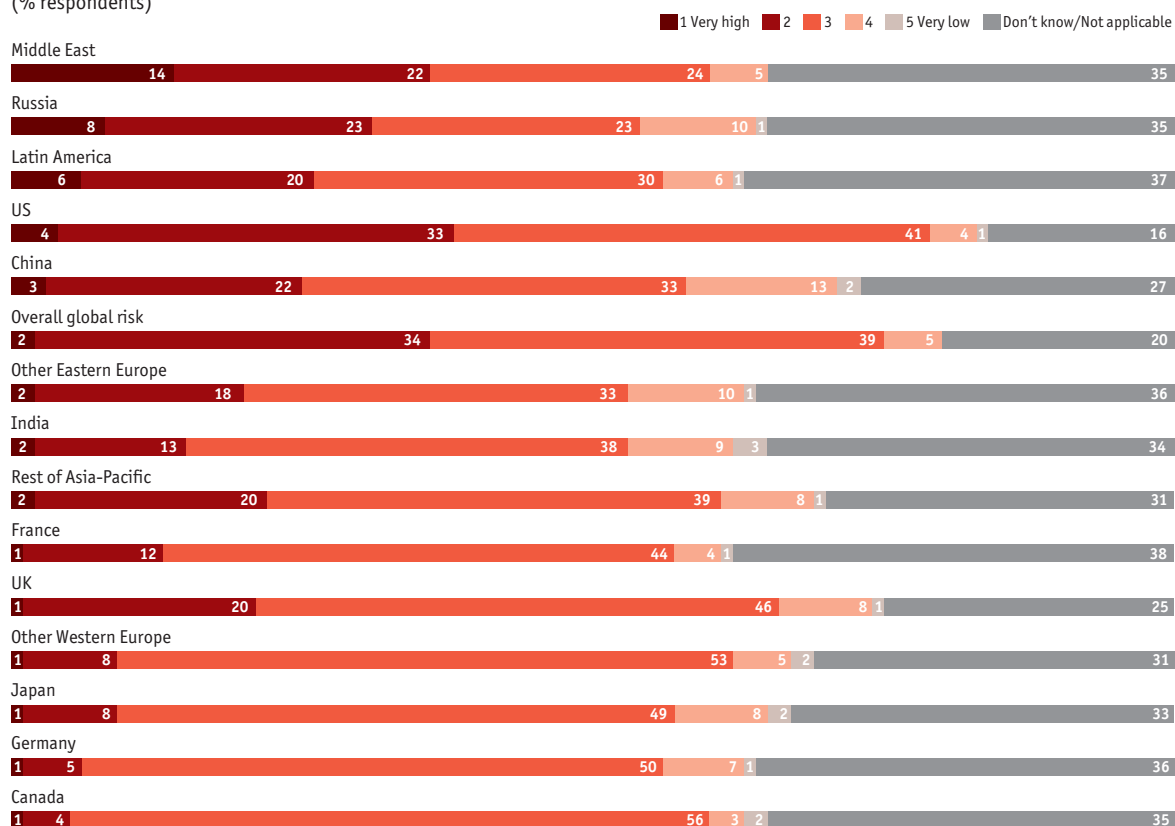


In each of the following regions, are the majority of risks to your business considered to be general (e.g. likely to affect many other companies operating in the same location or industry) or specific (e.g. relating to your company's internal systems, processes or people)?

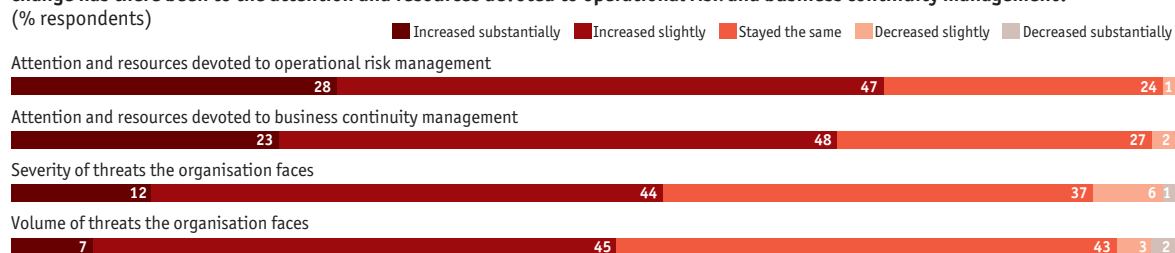
(% respondents)



How has your organisation's assessment of risk in each of the following countries and regions changed over the past three months?
(% respondents)



In the past three years, what change has there been to the number and severity of threats that the organisation faces, and what change has there been to the attention and resources devoted to operational risk and business continuity management?



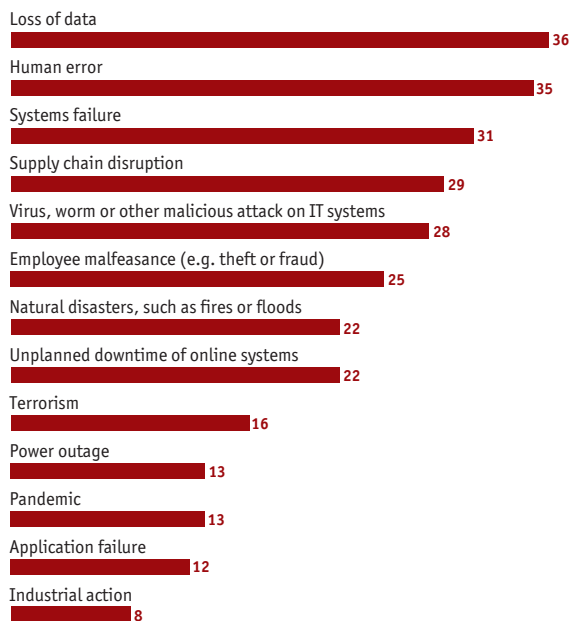
Appendix: Survey results

Business resilience

Reducing vulnerability and increasing preparedness

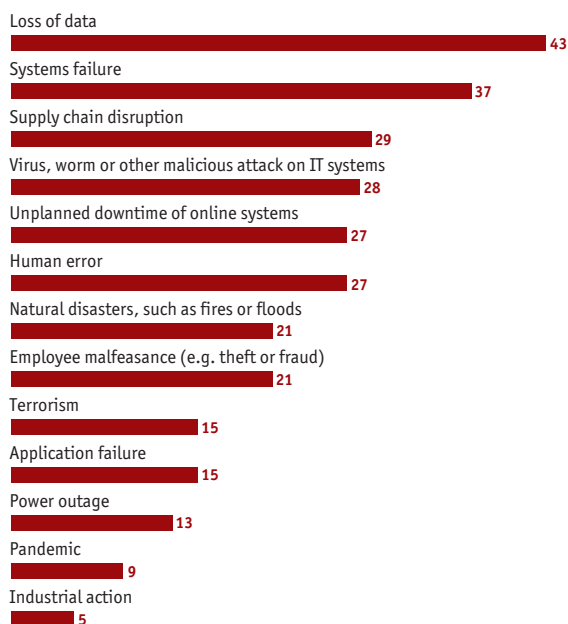
Which of the following types of threats are seen to be most important in your organisation's consideration of operational risk management planning?

(% respondents)



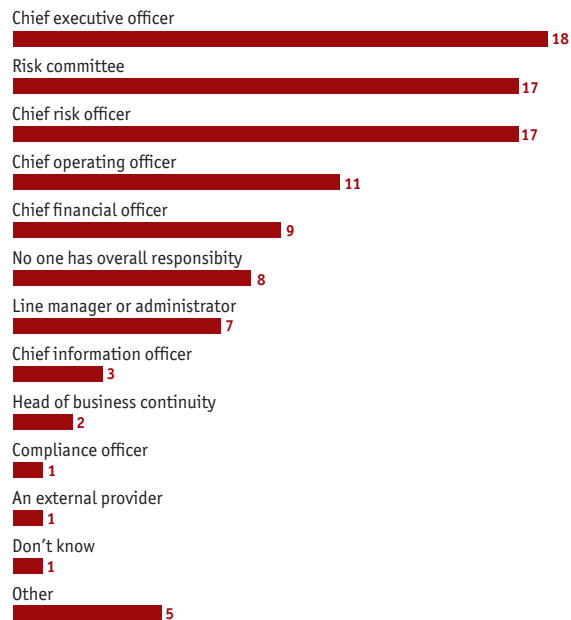
Which of the following types of threats receive most attention in your organisation's consideration of operational risk?

(% respondents)



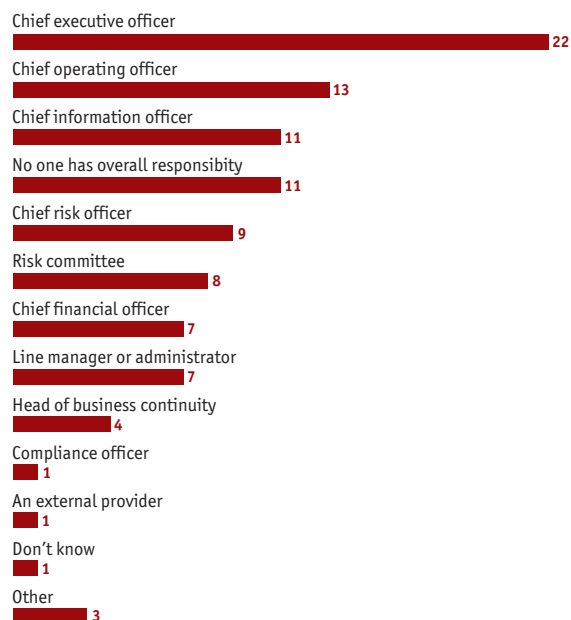
Who is primarily responsible for operational risk in your organisation?

(% respondents)

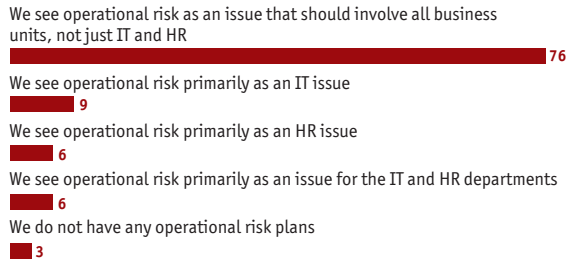


Who is primarily responsible for business continuity planning in your organisation?

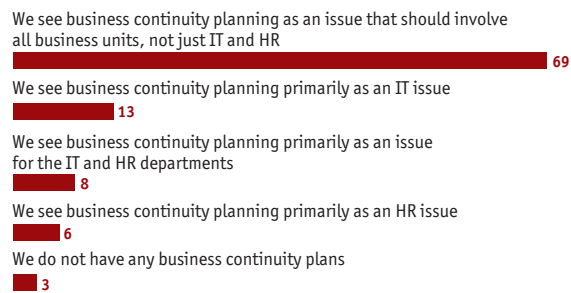
(% respondents)



Which of the following statements best describes your organisation's approach to operational risk planning?
(% respondents)



Which of the following statements best describes your organisation's approach to business continuity planning?
(% respondents)

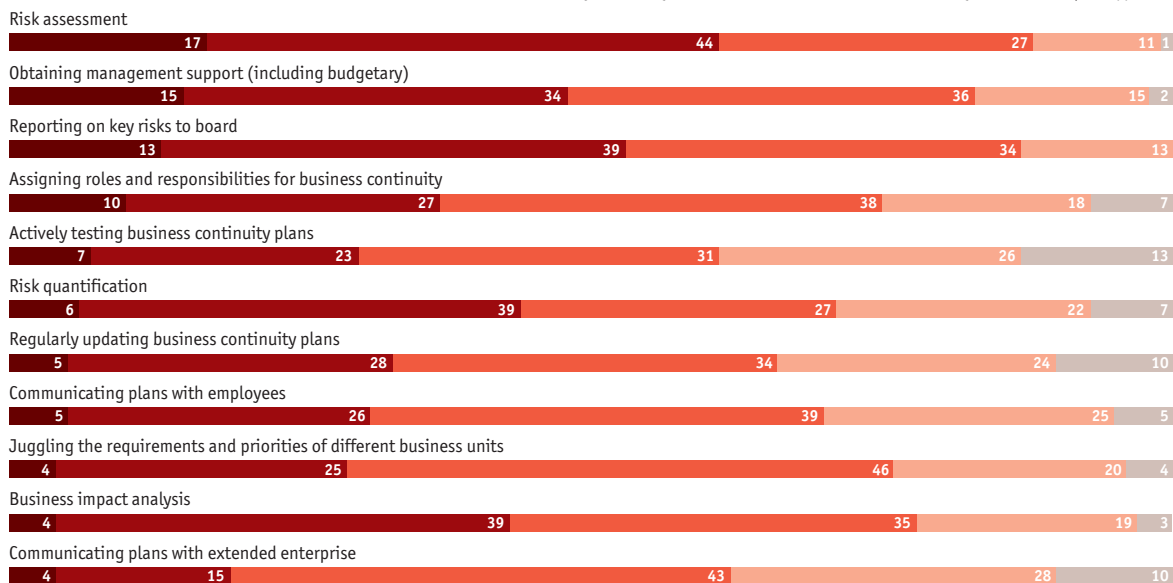


How successfully do you think your organisation manages the following aspects of operational risk?

Rate on a scale of 1 to 5, where 1=Very successfully and 5=Not at all successfully.

(% respondents)

1 Very successfully 2 3 4 5 Not at all successfully Don't know/Not applicable



Appendix: Survey results

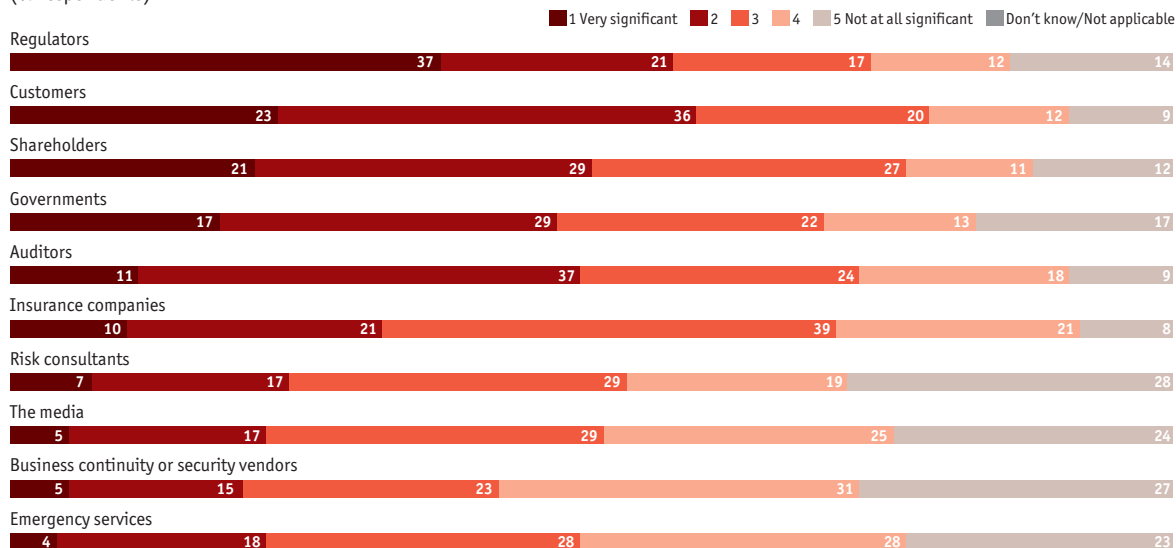
Business resilience

Reducing vulnerability and increasing preparedness

How significant is the influence that the following external organisations have over your decisions about business continuity planning?

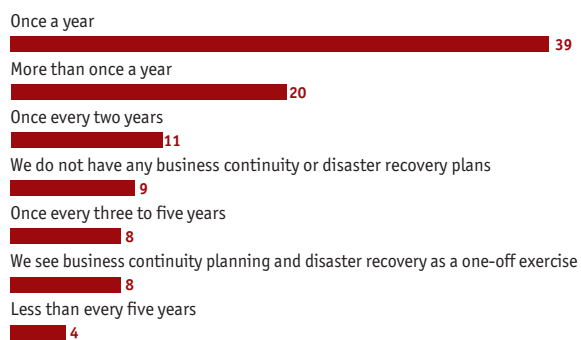
Rate on a scale of 1 to 5, where 1=Very significant and 5=Not at all significant.

(% respondents)



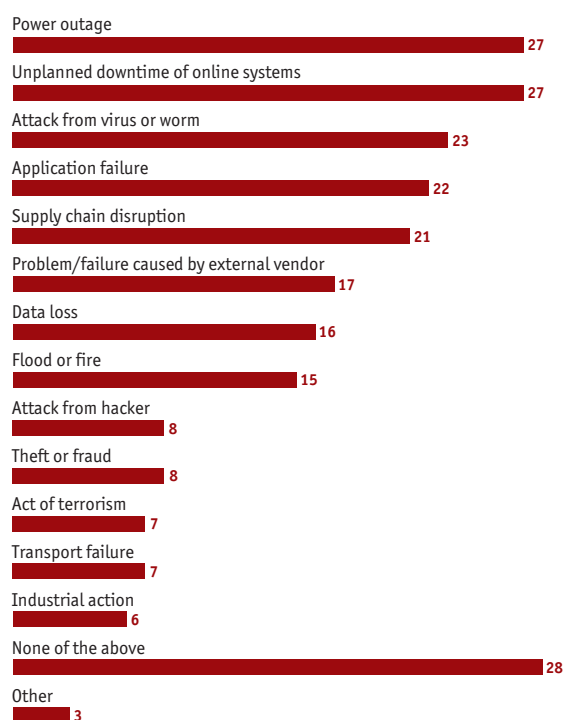
How often do you update and actively test your business continuity and disaster recovery plans?

(% respondents)



In the past year, which of the following incidents has caused you to put into action your business continuity plans?

(% respondents)



Please indicate whether you agree or disagree with the following statements:

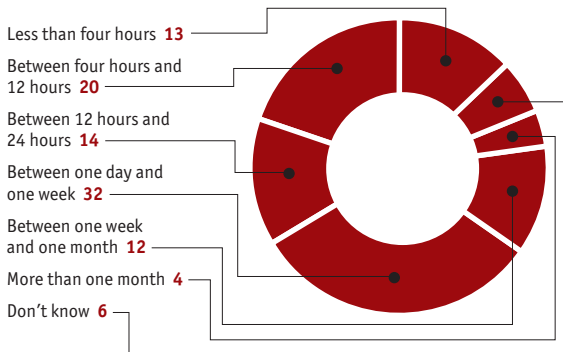
(% respondents)

■ Strongly agree
 ■ Slightly agree
 ■ Neither agree nor disagree
 ■ Slightly disagree
 ■ Strongly disagree
 ■ Don't know



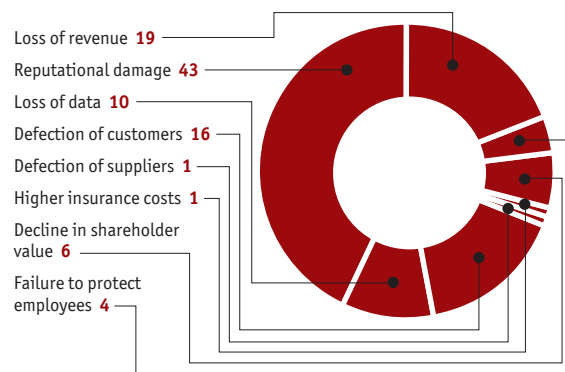
How long could your organisation last before downtime of IT systems becomes an issue that could jeopardise the entire company?

(% respondents)



What do you see as being the biggest threat arising from poor business continuity planning?

(% respondents)

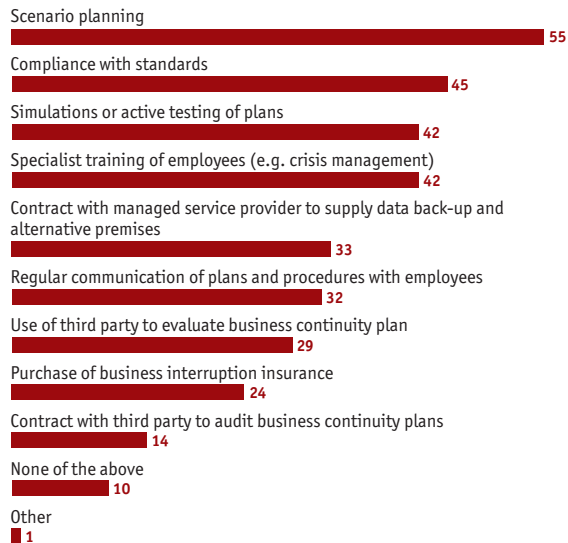


Appendix: Survey results

Business resilience

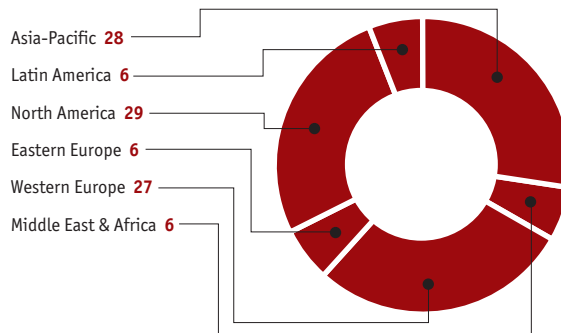
Reducing vulnerability and increasing preparedness

Which of the following methods does your organisation use to develop and test its business continuity plans? (% respondents)

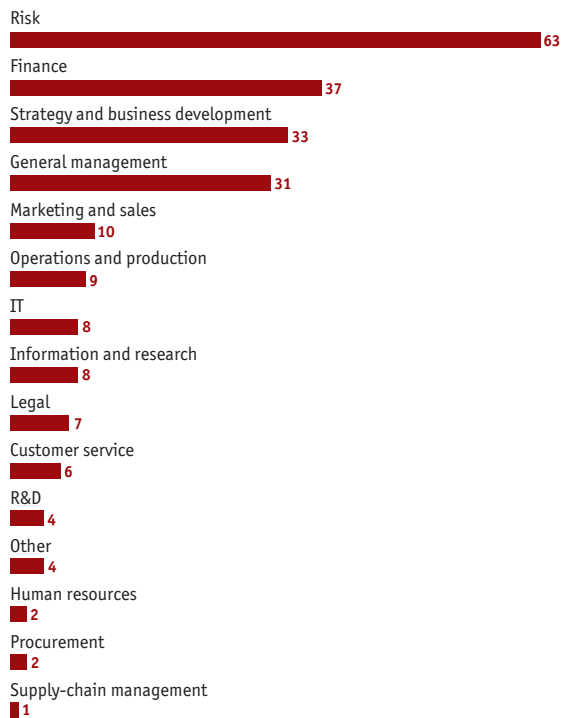


Demographics

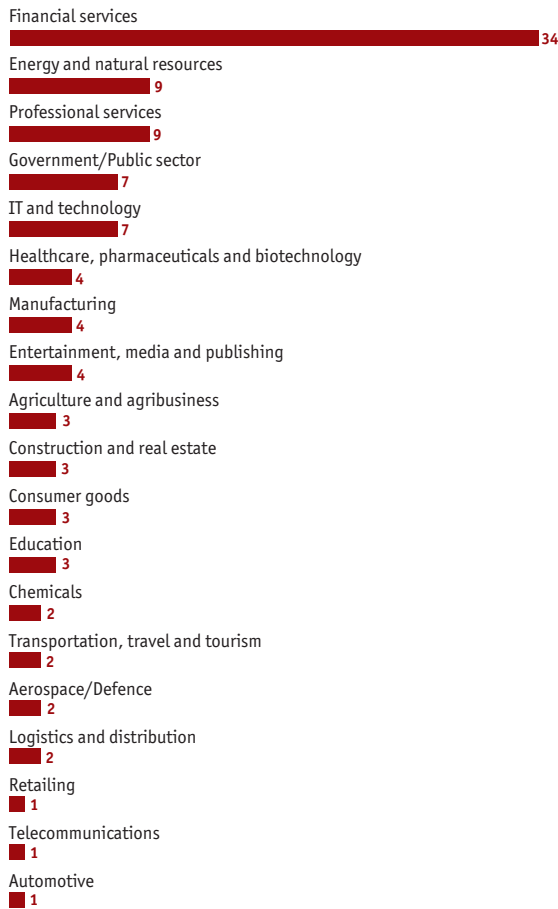
In which region are you personally located? (% respondents)



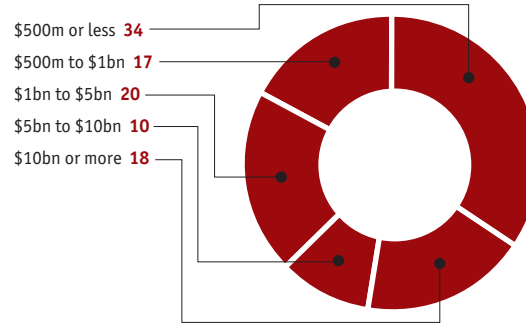
What are your main functional roles? Please choose no more than three functions. (% respondents)



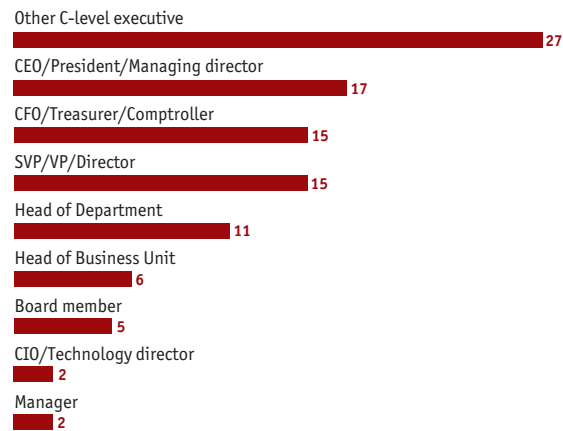
What is your primary industry?
(% respondents)



What are your organisation's global annual revenues in US dollars?
(% respondents)



Which of the following best describes your title?
(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

LONDON
26 Red Lion Square
London
WC1R 4HQ
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

NEW YORK
111 West 57th Street
New York
NY 10019
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
60/F, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com