Economist Intelligence Unit | The Economist

Natural catastrophes: business risks and preparedness
A research programme sponsored by Zurich Insurance Group
Executive summary
March 1st 2013

About the survey

The survey, conducted in January 2013, included responses from 170 executives from around the world. Of them, 49% are C-level executives or board members, and another 28% are other senior executives (senior vice-president, vice-president, director, head of business unit or department). About one-third of respondents are located in the Asia-Pacific region, with nearly 30% each from North America and Europe. The remaining 9% are located in Latin America, the Middle East and Africa. Respondents are almost equally split between companies with less than US$500m in annual global revenue and those with higher revenue. Nearly one-quarter are from companies with revenue of $10bn or more. The survey covers 19 different industries, with the largest representation from professional services (15%), financial services (11%) and IT/technology (11%). About 6% are from the government/public sector.

Overview

The survey confirms a widespread perception among organisations that natural catastrophes are becoming both more frequent and more severe, and that commensurate importance is assigned to assessing and mitigating the associated risks. Survey respondents say that business disruption from a natural catastrophe would encompass multiple aspects of the enterprise, with the most severe threats confronting supply-chain logistics and continuity of IT support.

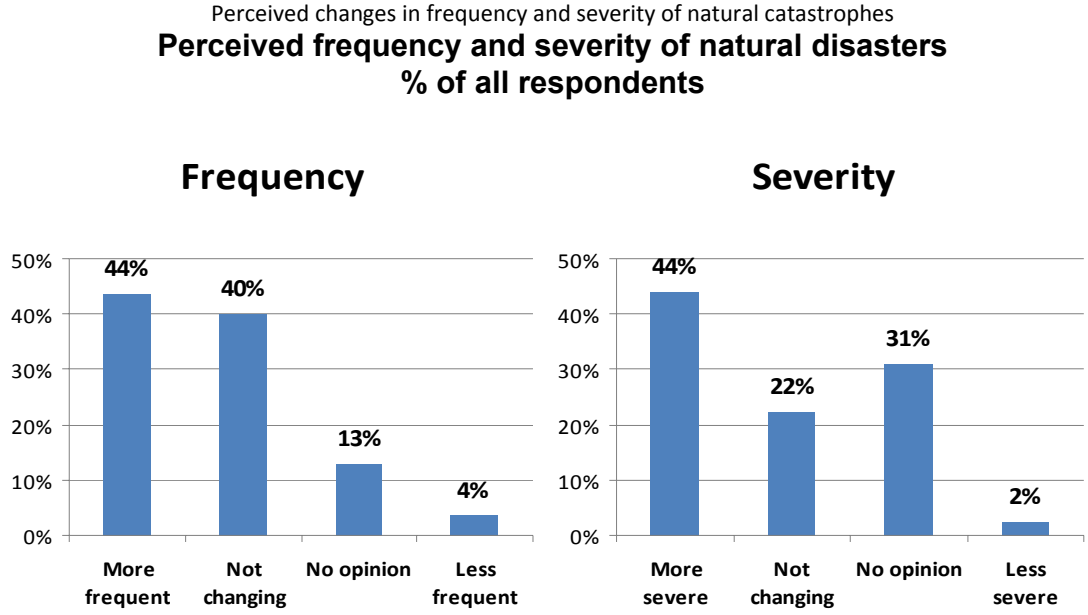
The research suggests that there is significant room for improvement in companies' planning and continuity endeavours. This is true for business-critical functions and is a serious concern for many companies' IT functions in particular. Although most companies in this survey have taken some steps to mitigate associated threats to IT systems, the adoption of systematic, integrated approaches to risk management is surprisingly low. Only a minority of companies use some form of scenario analysis to assess the risks of natural catastrophes. Moreover, while a large majority say that they have addressed the challenges of mitigating IT risks from natural catastrophes, only 31% say that their risk-management strategy explicitly addresses the interconnectedness of different types of risk. The findings suggest that while businesses are aware of the challenges they face, most have not yet developed a holistic approach to confronting these risks.

Key findings

1: Natural catastrophes are perceived as a growing threat and are receiving considerable attention from business enterprises.

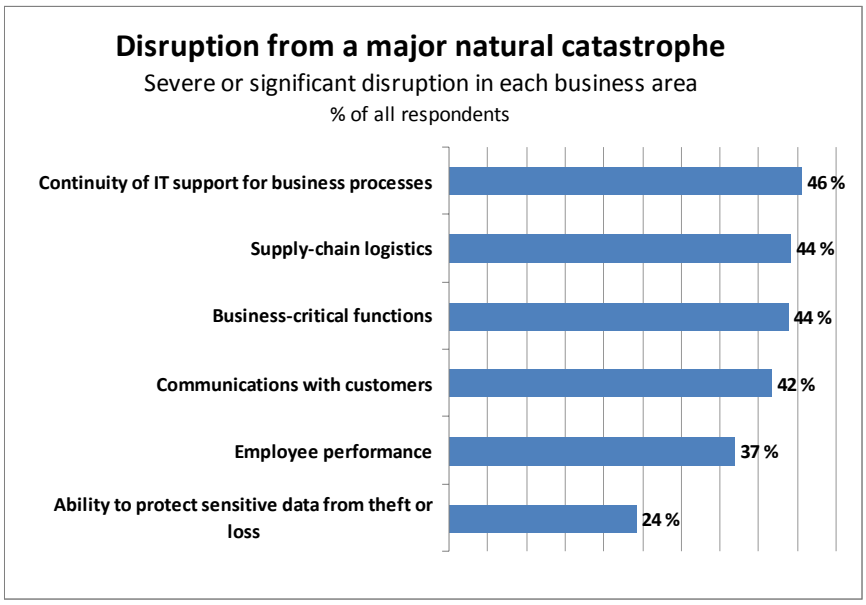
The predominant view of respondents is that natural catastrophes are becoming more frequent and more severe, with 44% agreeing in each case. Only a handful perceive the opposite trends, while 40% and 22% respectively say that frequency and severity remain about the same as in the past. However, relatively large groups of respondents did not express an opinion about frequency (13%) or severity (31%).

Perceived changes in frequency and severity of natural catastrophes

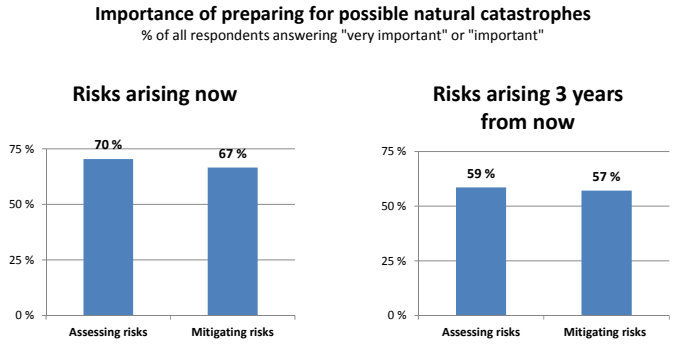


Survey respondents were asked to rate the severity of potential disruptions to distinct areas of their business operations in the event of a natural catastrophe occurring within the next three years. Combining the top two most severe ratings on a scale of five puts continuity of IT support as facing the most severe disruption (46%), followed by supply-chain logistics (44%) and business-critical functions (44%). The ability to protect sensitive data from theft or loss is regarded as the business area least prone to disruption, with only 7% predicting severe disruption.

Supply-chain logistics are difficult to address in the event of a natural catastrophe, as they are generally outside of an organisation's immediate control. Despite this, other business areas, including core business functions, are in line with supply-chain concerns. The core of business continuity consists of buttressing business-critical functions, but such functions are as likely to be significantly disrupted as supply chains or IT support. Taken together, these findings indicate that there is plenty of room for improvement. One hopeful finding is that security of sensitive data is associated with a lower risk of disruption. This may be a sign that companies are taking steps to protect their core IT assets even in the face of natural disasters.



Businesses' actions do not reflect the high degree of importance that respondents assign to preparing for natural catastrophes. Current risks are seen as somewhat more important than risks that will arise over the next three years. About 70% of respondents say that assessing current risks is important or extremely important, and nearly as many (67%) say the same about mitigating current risks. Looking to the next three years, smaller majorities rate risk assessment (59%) and risk mitigation (57%) as highly in importance.

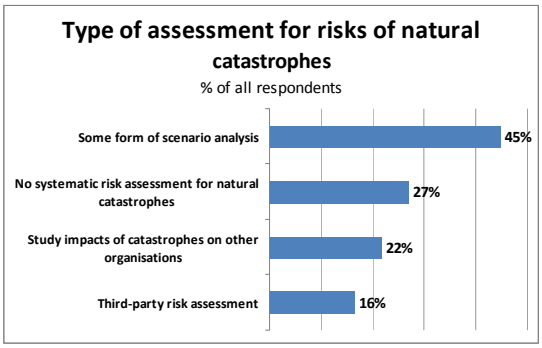


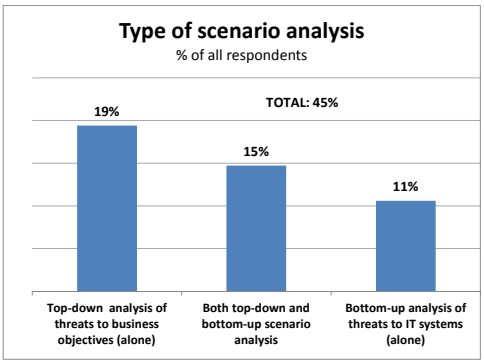
2: Only a minority of organisations use systematic scenario analysis to assess the risks of natural catastrophes.

Fewer than half of survey respondents (45%) say that they use some form of scenario analysis to assess the risks of natural catastrophes. This includes companies that use top-down scenario analysis of threats to key business objectives (19%), bottom-up scenario analysis of threats to IT systems (11%) or both types (15%). Another 16% use third-party risk assessments, but nearly three in ten (27%) say that they do not systematically assess business risks related to natural catastrophes.

Under one-quarter (22%) of respondents say that their company studies the impact of previous natural catastrophes on other organisations. Notably, only 28% of all respondents say that their company uses the results of scenario analysis to integrate natural catastrophes into a comprehensive business-continuity plan, although 18% use it to support plans for distinct catastrophic events. Thus, while scenario analysis in its various forms is widely used, the majority of respondents say that their organisation does not use it to assess the risks of natural catastrophes. In fact, roughly half of those who do not use scenario analysis say that they do not systematically assess risks of natural catastrophes at all.

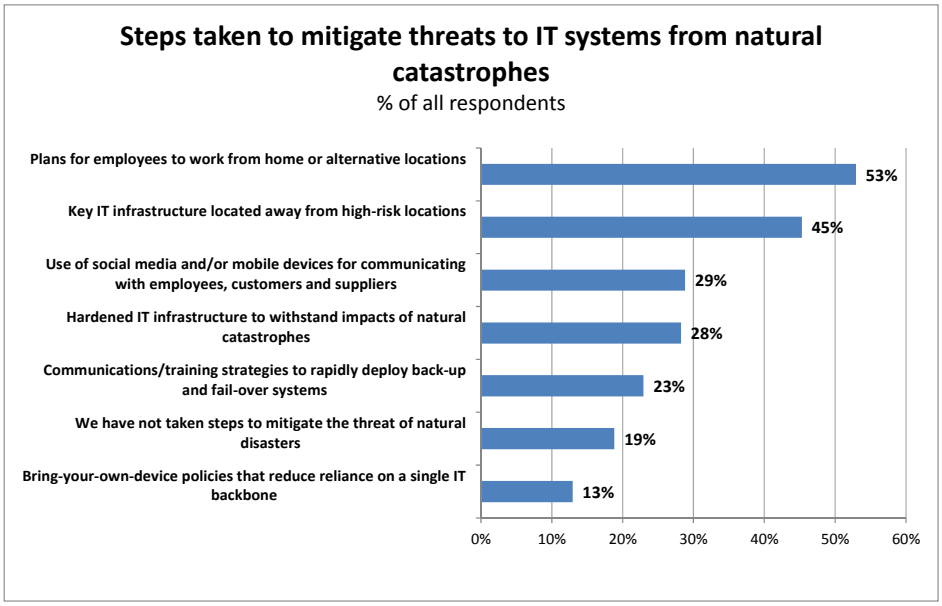
This means that many companies are unprepared for natural disasters despite being aware of their severity. Inadequate budgets are the most common obstacle standing in the way of more effective risk management, so this may be a question of short-term investments being favoured over long-term stability. However, a lack of technical risk-management skills and the inability to present compelling business cases have also been cited as important hurdles.





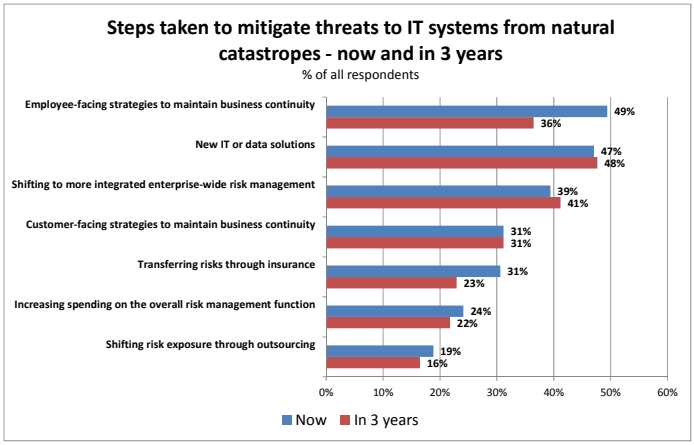
3: One in five companies have taken no steps to mitigate threats to IT systems from natural catastrophes.

Nearly one- fifth (19%) of companies have not adopted any strategy to mitigate IT risks related to natural catastrophes. About two-thirds (66%) of respondents say that their companies have adopted at least one of three hardware-orientated strategies for mitigating threats to IT systems in the event of a natural disaster. These include locating IT infrastructure away from high-risk regions, hardening IT infrastructure against physical disruption and adopting early-warning tools for back-up or fail-over systems. However, only 21% of companies have adopted two of these strategies and a mere 5% use all three. Nearly as many companies (62%) have adopted employee-focused strategies as hardware approaches. These include working from home or alternative locations, using social media or mobile devices, and bring-your-own device policies. Here again, one-fifth (21%) have adopted two of these employee-related strategies, but only 6% use all three.



Clearly most businesses are trying to be proactive in some form, but only a tiny minority are employing the full gambit of robust risk-mitigation tools available to them. More broadly, the companies represented in this survey have also adopted a wide range of approaches for managing the full range of business risks they face. Employee-facing business-continuity strategies such as work-at-home and bring-your-own-device (49% of all respondents) were slightly favoured over new IT or data solutions (47%) when it comes to the means of risk mitigation, but this is likely to reverse as employee-facing solutions are expect to decline to 36% over the next three years.

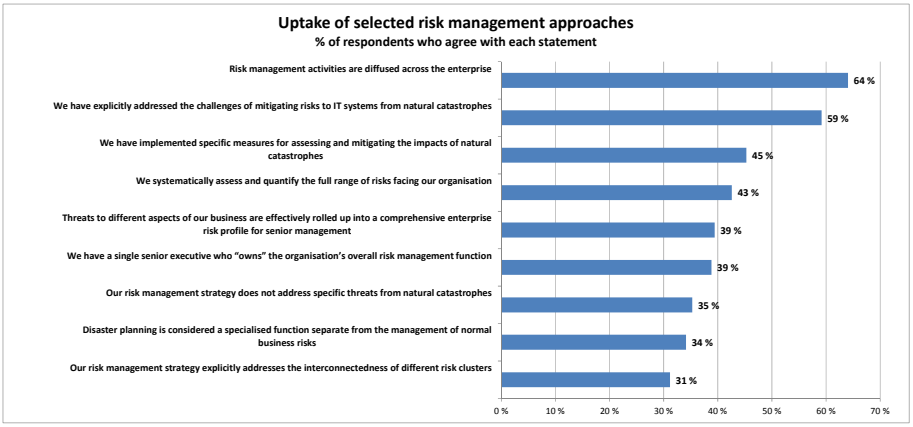
Crucially, less than two-fifths (39%) have adopted enterprise-wide risk management. This cannot be only a question of resources, as even among companies with over $500m in annual revenues, only 57% have moved to such integrated risk management. A minority of companies are transferring risk through insurance (31%) frequently to bolster their own enterprise risk-management endeavours.



4: Efforts to address the interconnectedness of risk clusters through integrated risk management have been only partially successful.

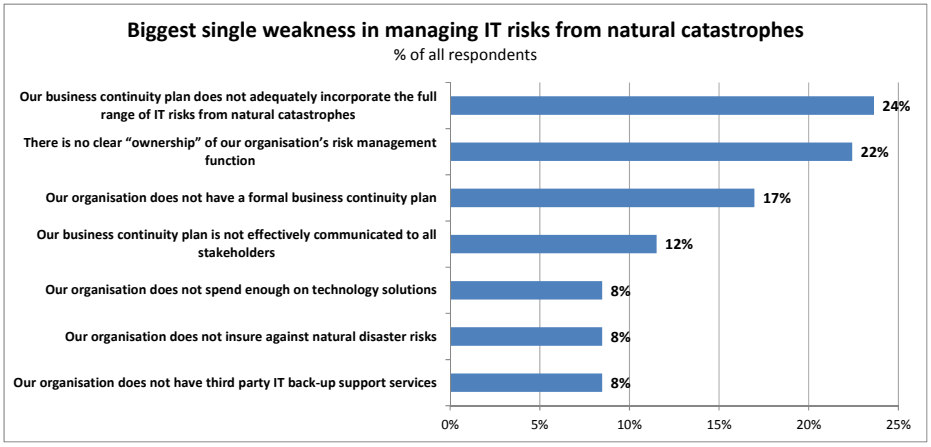
Survey respondents point to mixed results in addressing the interconnectedness of different risk clusters. More than twice as many (59%) agree than disagree (28%) that their company has explicitly addressed the challenges of mitigating risks to IT systems from natural catastrophes. But they are divided (39% to 39%) on whether different risks are effectively rolled up into a comprehensive risk profile for senior management and also (43% to 40%) on whether the company systematically assesses and quantifies the full range of risks. Only 39% agree that a single senior executive "owns" the overall risk-management function and less than one-third (31%) say that their company's risk-management strategy explicitly addresses the interconnectedness of different risk clusters.

The survey suggests that progress has been made in recognising risks from natural catastrophes. However, a full integration of risk management across the enterprise remains spotty. Although a long-term trend towards integrated enterprise-wide risk-management programmes has been documented, progress remains slow.

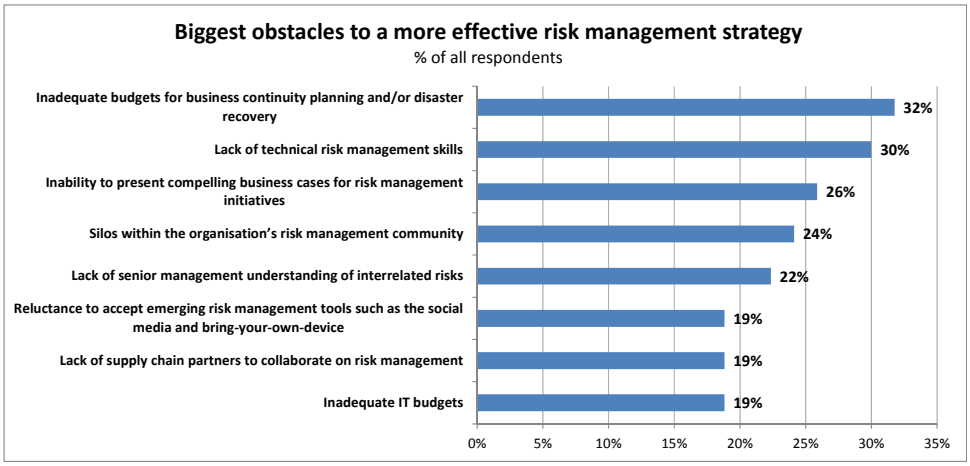


5: Inadequate integration of risk categories is the most significant weak point in managing IT risks from natural catastrophes.

When asked to name the single biggest weakness in their company's strategy for managing IT risks from natural catastrophes, nearly one-quarter (24%) of respondents point to the failure to incorporate the full range of risks into the business-continuity plan. This is followed closely (22%) by the lack of clear ownership of the organisation's risk-management function. The only other weaknesses to attract more than 10% of responses are the lack of a formal business-continuity plan (17%) and the failure to effectively communicate the business-continuity plan to stakeholders (12%). These are leadership failings of one form or another, identified by the senior executives themselves.



Respondents consider inadequate budgets for business-continuity planning and/or disaster recovery as the biggest obstacle to adopting more effective risk-management strategies. Given the still-shaky return to growth in many markets this is perhaps understandable, but ultimately problematic. About one-third (32%) chose this as one of three responses, compared with 30% who cited the lack of technical risk-management skills. An inability to present compelling business cases for risk-management initiatives (26%) and silos within the organisation's risk-management community are other significant hurdles. These obstacles can present a challenge to business leaders when it comes to putting their own houses in order.



There is a strong propensity for companies where a single executive owns the overall risk-management function to report success in integrating risk management across the organisation. Such companies are nearly twice as likely (42% agree and 24% disagree) to say that their risk-management strategy explicitly addresses the interconnectedness of different risk clusters. They are also far more likely (62% versus 32%) to report that "we systematically assess and quantify the full range of risks facing our organisation" and have higher success rates (71% versus 51%) in explicitly addressing the challenges of mitigating risks to IT systems from natural catastrophes.

Conclusions

This survey confirms that organisations face challenges in developing comprehensive enterprise-wide risk-management strategies. A key element of such a strategy would be a full integration of threats from natural catastrophes into the organisation's systems for identifying, assessing and controlling risks. While the survey found that many organisations are taking action in these directions, this analysis concludes that considerably more effort will be required before the risks of natural catastrophes are adequately controlled.

Particularly important progress has been achieved in the area of IT risk-mitigation strategies. Nearly 80% of respondents say that their organisation has adopted at least one hardware-focused and at least one employee-focused IT risk-management strategy related to natural catastrophes. And nearly 60% say that these initiatives have been largely successful. Yet efforts to address the interconnectedness of risk clusters through integrated risk management remain incomplete, as only a minority of business have developed a comprehensive risk profile for senior management.

A lack of adequate resources or technical know-how is the most common reason for organisations' failure to build more integrated risk-management strategies. But access to resources is a matter of priority. It is significant, therefore, that many respondents lack the ability to present a compelling business case for risk-management initiatives. But, while rigorous analysis for mitigation strategies may provide clearer metrics to inform decision-making, the onus is on senior executives to own the risk strategy in a comprehensive way if businesses are to become truly better prepared.