

HORIZON SCAN 2012

BCI Survey Published January 2012

Global business continuity concerns are driven by IT and Internet vulnerabilities in 2012.



Dominating the horizon scanning of business continuity professionals around the world are threats arising from IT, telecom and Internet dependencies.

The top threats evaluated through risk assessment, based on those registering *extremely concerned* and *concerned*, include the following:

- Unplanned IT and telecom outages
- Data breach (i.e. loss or theft of confidential information)
- Cyber attack (e.g. malware, denial of service)

It would be wrong, however, to push these threats down to IT departments to deal with. Data breaches and cyber attacks have far reaching reputational and compliance consequences. Cyber attacks might be incurred as a result of more strategic business issues (a modern form of boycott or retaliatory measures for perceived business ethic violations) as well as attempts to steal information. Additionally, regulators such as the US Securities and Exchange Commission are formalising their disclosure requirements in relation to cyber security risks and cyber incidents.

The survey results also show that business continuity practitioners are applying BCM to a far wider range of threats than those with which the discipline is traditionally associated. For example, *Business ethics incident*, *new laws and regulations*, the *availability of credit* and *exchange rate volatility* all feature in the planning of BCM practitioners.

This should not be a surprise given that *business resilience* requires a comprehensive approach, one that BCM offers. BCM provides the link between the organization's objective, the risks that it agrees to take, and the measures needed to manage the resulting vulnerabilities.

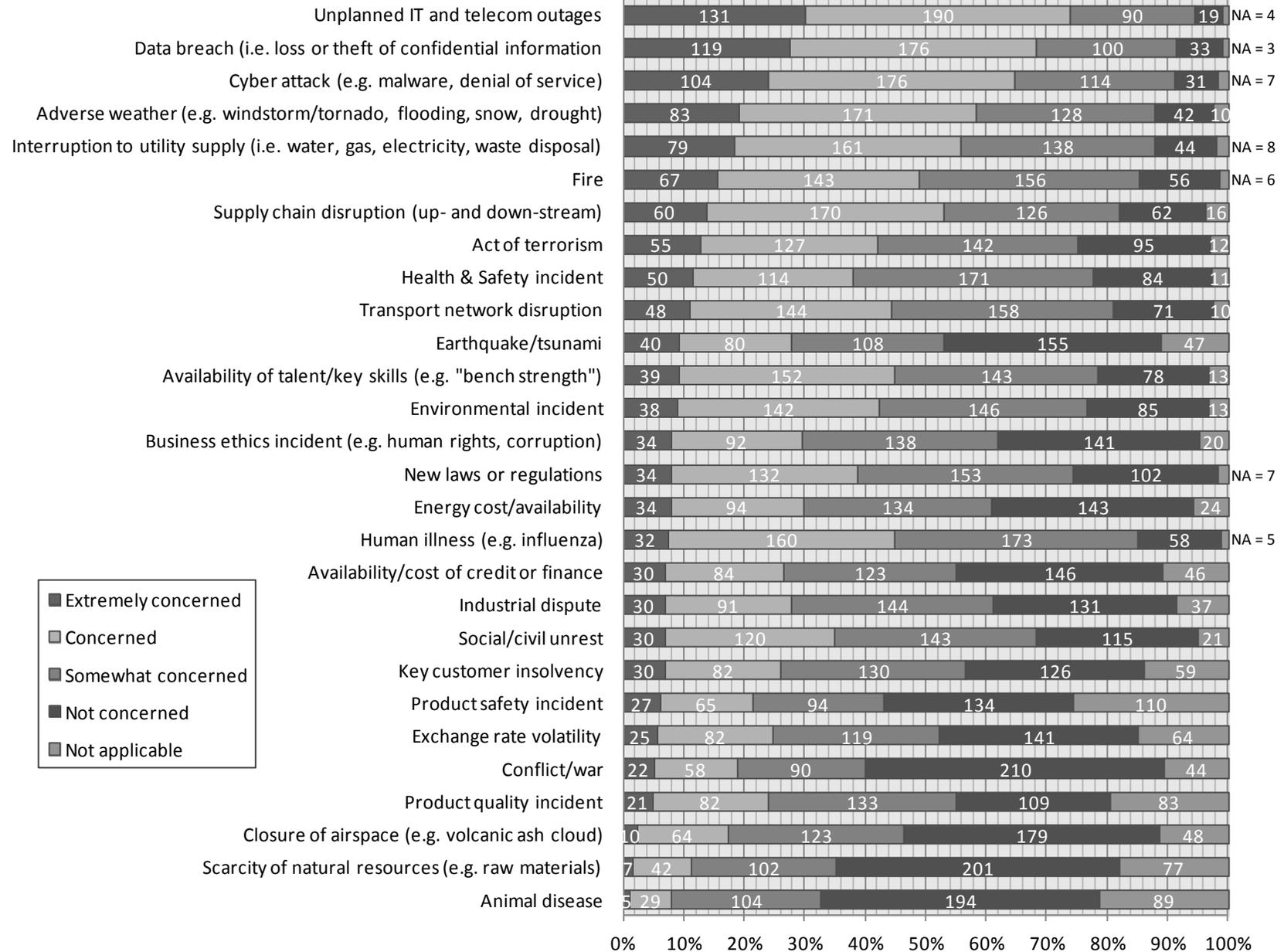
The survey does raise a question as to the extent that individual organisations can deal with these challenges by themselves and the extent to which shifts in public policy are required in order to help businesses. Dealing with the world as it is, BCM can help with exploring alternative strategies in business execution, but governments can do more to mitigate the threat environment through closer international co-operation around critical global infrastructures.

The top five threats evaluated through risk assessment, based on those registering *extremely concerned* and *concerned*, are as follows:

- Unplanned IT and telecom outages – 74%
- Data breach (i.e. loss or theft of confidential information) – 68%
- Cyber attack (e.g. malware, denial of service) – 65%
- Adverse weather (e.g. windstorm/tornado, flooding, snow, drought) – 59%
- Interruption to utility supply (i.e. water, gas, electricity, waste disposal) – 56%

Additional and/more specific risks identified by respondents included: Impact of the 2012 Olympics, raw material prices, social networking (reputational damage), escalation of the euro financial crisis and vandalism/theft.

Based on your analysis, how concerned are you about the following threats to your organization in 2012?



Base: 458. Multiple responses allowed.

Copyright ©The Business Continuity Institute 2012

Based on your analysis, how concerned are you about the following threats to your organization in 2012 (Scale 1-4)

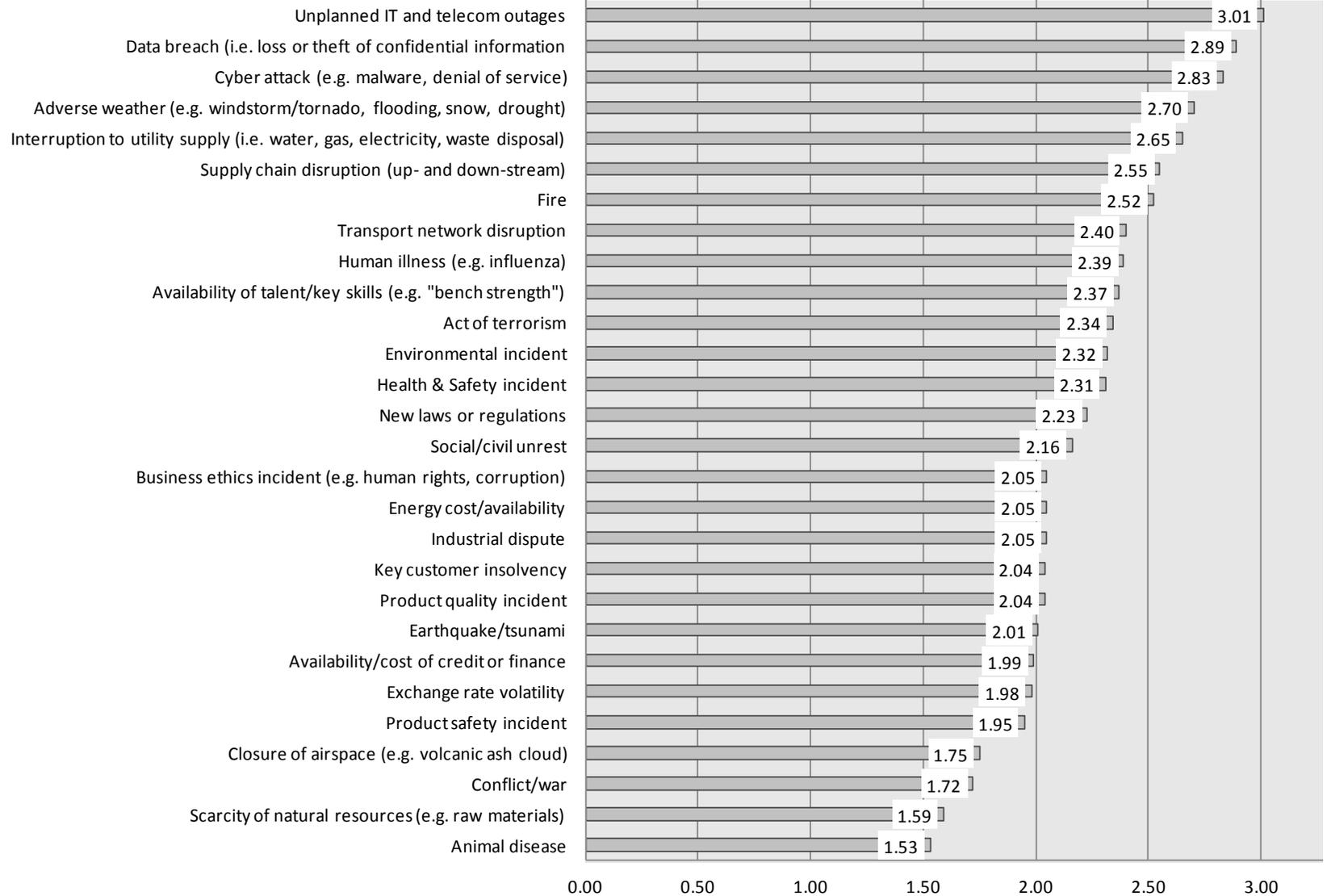
In this chart, each threat is evaluated against scale which translates into a score as follows:

- Extremely Concerned: 4
- Concerned: 3
- Somewhat concerned: 2
- Not concerned: 1

Note: *not applicable* is available as a non-scoring choice.

The highest score would be 4.00 which would equate to 100% of respondents for whom the threat is applicable marking it as *extremely concerned*.

This approach has generated some differences further down the scale where *somewhat concerned* numbers are a significant proportion. For example, *human illness* scores 2.39 or 9th position under this scoring method rather than 17th.



Threat evaluation by primary activity of the organization (SIC 2007 sectors)

While there is general consensus around key threats in financial services, information and communications, and professional services, manufacturing places supply chain disruption as their focal point, while *human illness* reaches the top three among public administration sector respondents.

The extent of cross-sector dependencies on underlying IT and Internet infrastructures is otherwise the notable finding from this survey.

Other sectors covered within the overall survey response are *health & social care, education, retail/wholesale, engineering/construction, entertainment and leisure, transport and storage, support services, mining and quarrying, and agriculture, forestry and fishing.*

Sector	Top 3 Threats	“Extremely Concerned” plus “Concerned” (%)	Average score across the full scale (1= not concerned; 4 = extremely concerned)
Financial Services (Base = 124)	<ul style="list-style-type: none"> Unplanned IT/telecom outage Cyber attack Data breach 	80% 71% 68%	3.15 2.99 2.90
Information & Communications (Base = 77)	<ul style="list-style-type: none"> Unplanned IT/telecom outage Data breach Cyber attack 	81% 77% 75%	3.11 3.14 3.01
Professional Services (Base = 70)	<ul style="list-style-type: none"> Data breach Unplanned IT/telecom outage Cyber attack 	66% 65% 60%	2.82 2.87 2.83
Public Administration (Base = 43)	<ul style="list-style-type: none"> Adverse weather Unplanned IT/telecom outage Human illness 	74% 60% 60%	2.86 2.76 2.64
Manufacturing (Base = 17)	<ul style="list-style-type: none"> Supply chain disruption Unplanned IT/telecom outage Product safety incident 	76% 71% 53%	3.00 2.82 2.71
Health and Social Care (Base = 17)	<ul style="list-style-type: none"> Adverse weather Data breach Unplanned IT/telecom outage 	69% 69% 63%	3.00 2.94 3.00
Utilities (Base = 17)	<ul style="list-style-type: none"> Cyber attack Adverse weather Interruption to utility supply 	82% 81% 77%	3.12 3.13 3.18

Threat evaluation by country of the respondent (top responses)

There is a remarkable consistency across geographical areas in terms of the threats under consideration. However, looking beyond those countries with higher response levels, there are some interesting deviations:

In India, *transport network disruption* was rated at 3.33, followed by *social/civil unrest* at 3.11. Third place belonged to *fire*, which scored 3.00.

In the United Arab Emirates (UAE) *availability of talent /skills* reached third place with a score of 2.88.

Not surprisingly in Japan, consideration of an *earthquake/tsunami* scored 3.38, in fact every respondent was either *extremely concerned* or *concerned*.

	Top 3 Threats	“Extremely Concerned” plus “Concerned” (%)	Average score across the full scale (1 = not concerned; 4 = extremely concerned)
UK (Base = 167)	<ul style="list-style-type: none"> • Unplanned IT/telecom outage • Data breach • Adverse weather 	71% 59% 58%	2.88 2.71 2.68
USA (Base = 78)	<ul style="list-style-type: none"> • Unplanned IT/telecom outage • Data breach • Adverse weather 	80% 78% 76%	3.22 3.11 3.03
Australia (Base = 44)	<ul style="list-style-type: none"> • Unplanned IT/telecom outage • Adverse weather • Data breach 	75% 68% 68%	2.98 2.74 2.67
Canada (Base = 23)	<ul style="list-style-type: none"> • Cyber attack • Data breach • Adverse weather 	65% 57% 57%	2.68 2.73 2.64
South Africa (Base =15)	<ul style="list-style-type: none"> • Unplanned IT/telecom outage • Data breach • Interruption to utility supply 	93% 87% 79%	3.43 3.33 3.07

In 2012, how will investment levels in Business Continuity Management compare to levels in your organization in 2011?

In difficult economic times it is positive to see that BCM investment is holding firm for a majority of respondents and increasing for 25% of them. For 10% it is a different story, facing budget cuts and greater pressures to deliver with fewer resources.

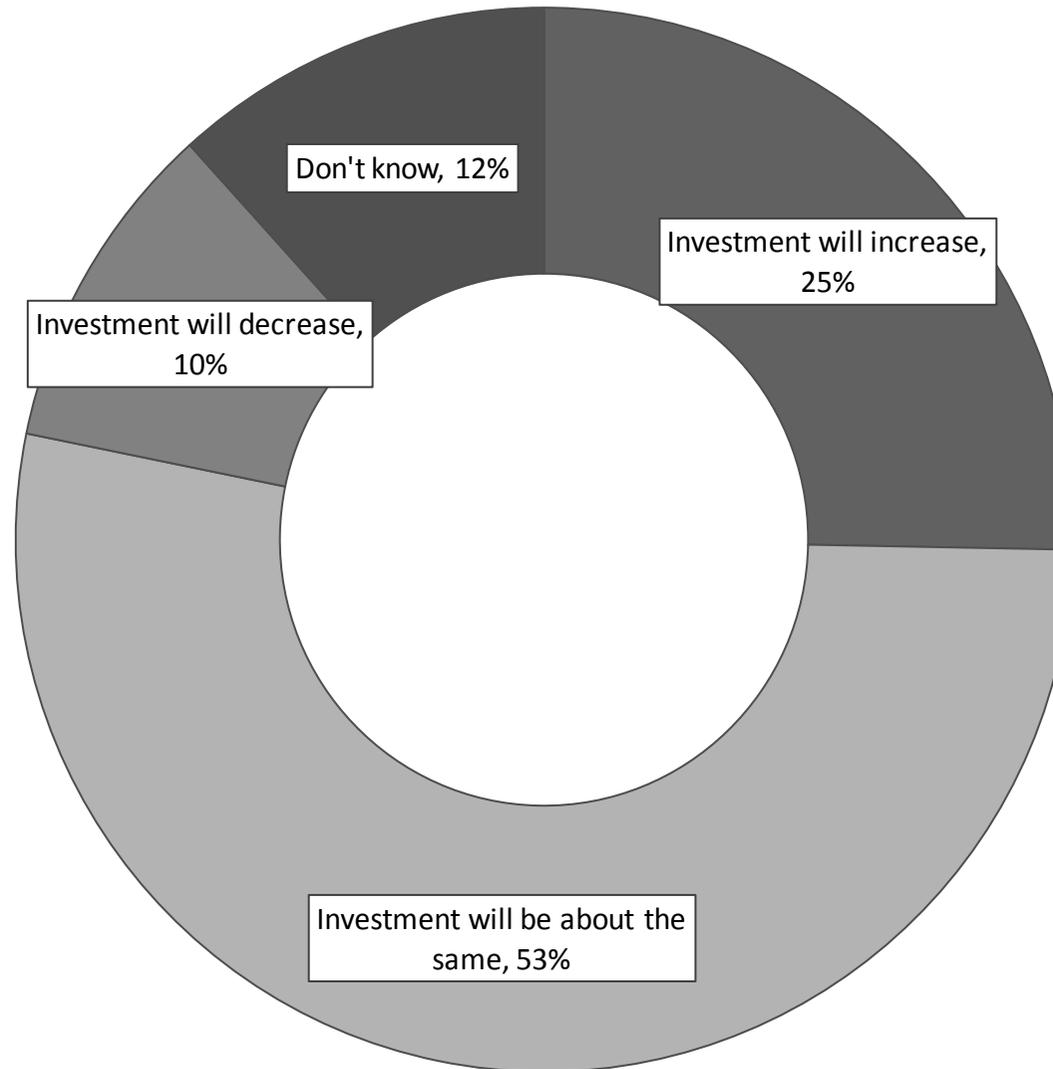
Comments from respondents:

“[I] have to fight for every penny”

“There is a 3% reduction across the board on operational budgets”

“The investment will be higher as a result of the Olympic Games”

“Looking to get more for the same investment”



Base: 454



About the survey

458 organizations responded to the online survey conducted from 5th to 20th December 2011. The question asked was: “Based on your analysis, how concerned are you about the following threats to your organization in 2012?” Respondents were asked to rate their level of concern against 28 identified threats. Respondents were drawn from 49 countries and 15 industry sectors.

For questions about the survey, contact Lee Glendon CBCI, lee.glendon@thebci.org

Copyright ©The Business Continuity Institute 2012