Business Continuity Institute

BCI SUPPLY CHAIN RESILIENCE REPORT 2017

ZURICH

Contents

Foreword BCI

The Business Continuity Institute is proud to present the ninth Supply Chain Resilience report, with the support of Zurich. This is one of our most mature and popular reports, as many professionals rely on it as a source of insight.

This survey captures different aspects of the supply chain industry, ranging from what threats organizations face to how they prepare for them. Given the international scale of this report, as supply chains usually involve operations in several countries, it is worth mentioning that the 408 respondents to this survey came from 64 different countries. This is key to understanding how similar threats might affect operations in different geographical regions.

Indeed, most of the vulnerabilities reported by respondents are transnational by nature. The top three causes of disruption are unplanned IT and telecommunications outages, cyber attacks and data breaches, and loss of talent, which affect organizations regardless of region, sector or size. Similarly, for the future ahead, professionals see the threat of international phenomena, such as terrorism, as some of their biggest concerns.

While there is still room for improvement in terms of building resilience to supply chain disruptions, there are steps in the right direction that have been consistent with previous reports, such as the growth of top management commitment towards the issue or the adoption of business continuity arrangements.

The renewed challenge posed by both physical and virtual origins of disruption underlines once more the need for collaboration among professionals with a different background and position within an organization. For example, information security, and business continuity managers could work together to determine the root of a cyber attack and ensure operations are kept running. Similarly, teams from business continuity and physical security could operate closely to mitigate the impact of a terrorist attack.

As respondents pointed out the challenges of getting different functions to work together, it is important to keep investigating how organizations can become more prepared and raise awareness about it. In this sense, this report aims to build knowledge that professionals can use to build more resilient supply chains.

David Thorp, Executive Director, BCI

Foreword, Zurich

In this interconnected and increasingly risky world, supply chain resilience is being recognised by many organizations as essential - and even a competitive advantage. This requires more responsive and responsible leadership, and collaboration both internally and externally with critical suppliers and associated regulatory bodies.

The BCI Supply Chain Resilience Report is one of the earliest and most comprehensive industry studies focusing on the origins, causes and consequences of supply chain disruption worldwide. It is now in its ninth edition and I know from talking to our customers and other industry contacts, it is seen as a very valuable resource.

The survey was completed during the period from June to early August 2017 so has not taken account of the tragic global weather events that have had further dramatic impacts on supply chains during the latter half of August and September. Produced by the BCI in association with global insurer Zurich, this study also benchmarks business continuity arrangements which raise the levels of resilience within organizations' supply chains. I would most importantly like to thank all of you who have invested the time to complete this survey - without your input the many benefits that have arisen from the research would not be possible.

I have been involved with the great team at the BCI and various Zurich colleagues in the development of the initial survey in 2009 and its ongoing evolution in terms of the provision of risk insights around Supply Chain Resilience. The benefits I have heard organizations getting out of this report include:

- Helping with the business case to senior management in terms of getting further investment to drive supply chain resilience - a key step in any Supply Chain Resilience programme
- Providing a framework and checklist in terms of what disruption areas to focus on
- Acting as a catalyst to help in a discussion to breakdown the functional silos to enable a cross-organizational approach

In the case studies this year we have included some thoughts on improving Cyber Risk management in the supply chain (a major cause of supply chain disruption) and a piece on a very useful tool the (Supply Chain Risk Maturity Model) which has been developed by the Supply Chain Risk Leadership Council.

At Zurich, we recognise the importance of supporting our customers in this complex risk area. Failures in Supply Chain Resilience can have a dramatic impact on organizational performance and having in place appropriate Business Continuity plans for critical suppliers is an important aspect of this. Zurich is able to offer services in this and other supply chain risk management areas, and we also share the risk with a number of our customers through our risk transfer solutions.

Nick Wildgoose, Global Supply Chain Product Leader, Zurich Insurance

Foreword, CIPS

These honest answers about the realities of supply chain disruption were both gratifying and alarming to read. Gratifying to understand what the key risks facing supply chains are and subsequently, the first step towards mitigating against them. However, as almost three quarters of respondents do not have full visibility of their supply chains, there are worrying signs too. I urge you to read the report as the data is worthy of deeper analysis about what other issues need to be unearthed.

Many businesses can be reluctant in putting the time and energy into business continuity unless there is an immediate benefit. It is often only when disruption hits that there is a more targeted focus on what the business needs. It can be viewed as a luxury when there appears to be no disaster looming on the horizon and the chances of something happening seem slim.

But that's where the danger lurks. Complacency, a lack of time, resources, and budget means that a lack of investment now increases the likelihood of a bigger disruption later. Usefully, this report offers some guidance on what that could be.

It's no surprise that IT and telecommunications outages, and cyber attacks have come to the top of the possible disruptions list. The number of these attacks increase with each passing year and are likely to become more widespread and more sophisticated in their approach. That is why every business needs to map their supply chains according to the impact on their own value and profitability so that there is a deeper understanding of the impact of disruption to a particular business in building an effective supply chain strategy.

Supply chain continuity must take into account both downstream (customer) and upstream (supplier) issues and there must be the right skills in place to do this efficiently. This assessed risk must be conducted along the entire length of the supplier chain from tier one to tier 20 if needs be and that's where companies get unstuck.

There is also only so much an organization can mitigate against. A company can pump budget and resources into internal infrastructures but external risks are so much harder to manage. Building strong relationships with suppliers and understanding their appetite for risk is also a big part of the work any business must do.

Wise supply chain managers should put business continuity at the core of their business operations along with risk, resilience, sustainability and ethics to keep operations running as smoothly as customers, partners, and staff expect.

Gerry Walsh, Group CEO, CIPS

1 Executive Summary

Executive Summary

Final number of respondents

408

Number of countries

64

69% do not have **full visibility** of supply chains

65% experienced at least 1 **supply chain disruption**

44% of disruptions occur at **Tier 1**

22% do not **analyse the source** of disruption

Top causes of disruption

Unplanned IT and telecommunications outage

Cyber attack and data breach

Loss of talent/skills

FIRE

is the biggest gainer at **7th** from **14th** last year

The following drop out of the top 10

9th to 11th: Act of terrorism

7th to 12th: Currency exchange volatility

Other sources of disruption emerge

14th to 7th: Fire

12th to 10th: Energy scarcity

Consequences of disruption

55% Down 13%: Loss of productivity

46% Down 7%: Increased cost of working

43% Up 3%: Customer complaints received

34% Down 6%: Service outcome impaired

32% Down 5%: Loss of revenue

31% Down 7%: Damage to brand reputation/image

Economic impacts of disruption

22% Report cumulative losses of at least one million euros

23% Report losses of at least one million euros due to a single incident

51% Do not insure for supply chain losses at all

Horizon scanning risks (next 12 months)

- Cyber attack and data breach
- Unplanned IT or telecommunications outage
- Loss of talent/skills
- TOP 10 — **Act of terrorism, product quality incident, and health and safety incident make it to the top ten this year**

Horizon scanning risks (next 5 years)

- Cyber attack and data breach
- New laws or regulations
- Unplanned IT or telecommunications outage
- TOP 3 — **New laws or regulations make it to the top three this year**

74% of organizations have business continuity arrangements in place to deal with supply chain disruptions

7% of organizations do not identify key suppliers

41% of organizations report strong top management commitment, up from 27%

2 Supply Chain Disruption

Supply Chain Disruption

Frequency and origins of disruption

There is a slight decrease (3%) in firm-wide reporting this year, from 34% to 31% (Figure 1). However, respondents confirmed a general upward trend, as the number of organizations that coordinate and report across the whole enterprise has increased from 23% in 2013 to 31% in 2017 (Table 1). While this is good news, there is still room for improvement as 31% have no reporting at all.

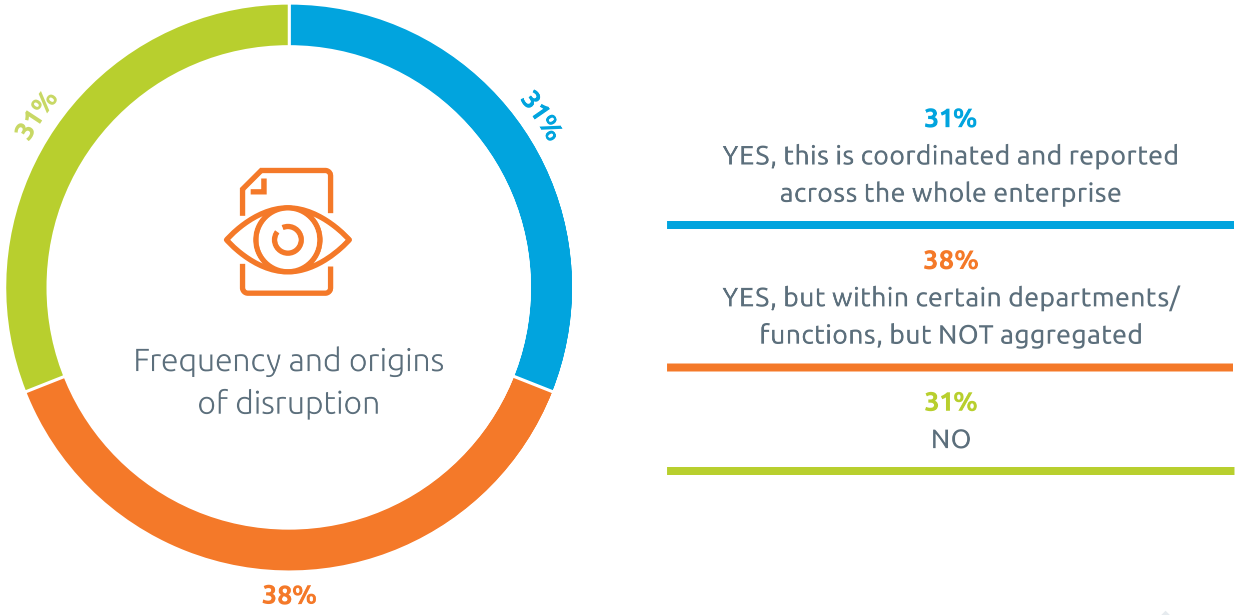


Fig 1: Question 6. Do you record, measure, and report on performance-affecting supply chain disruptions? (N=355)

Year	Firm-wide reporting	Reporting within certain departments	No reporting
2017	31	38	31
2016	34	38	28
2015	28	37	35
2014	27	40	33
2013	23	40	37

Table 1. Levels of reporting supply chain disruptions, in % (2012-2017)

Respondents share their thoughts.

“Identifying all non-business value wastes is essential in keeping the supply chain efficient and sustainable.”
“We’ve been asked to track potential financial losses based on incidents in the BCP department.”
“We have 37,000 nationwide vendors, although our procurement department doesn’t even know how many of them there are.”
“Disruptions will affect more than one section of the organization.”
“We do not report disruptions nearly as much as we should.”

It is interesting to observe that despite an increasing use of digital services by organizations, the majority (63%) do not use any technology such as risk analytics indicators to analyse, track or monitor the performance of their supply chains (Figure 2). There is variable uptake in terms of new solutions to supply chain management, even though in recent years there has been a move towards advanced analytics and forecasting[1].

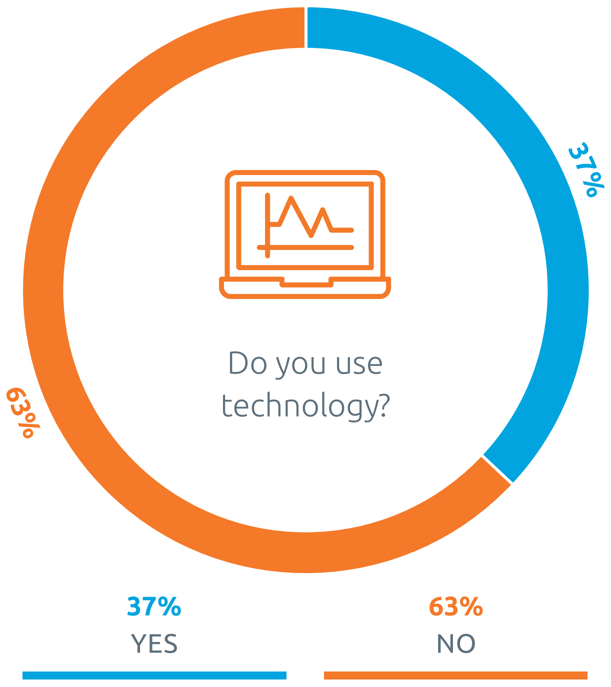


Fig 2: Question 7. Do you use technology (e.g. risk analytics indicators) to analyse, track or monitor potential performance-affecting supply chain issues that could cause disruptions? (N=352)

Out of those who utilise technology, 41% still rely on excel spreadsheets to keep track of supply chain disruptions (Figure 3). More specific solutions such as incident response data (13%), third party due diligence solutions (10%), BCM software (9%) and financial solvency models (5%) complete the top five.

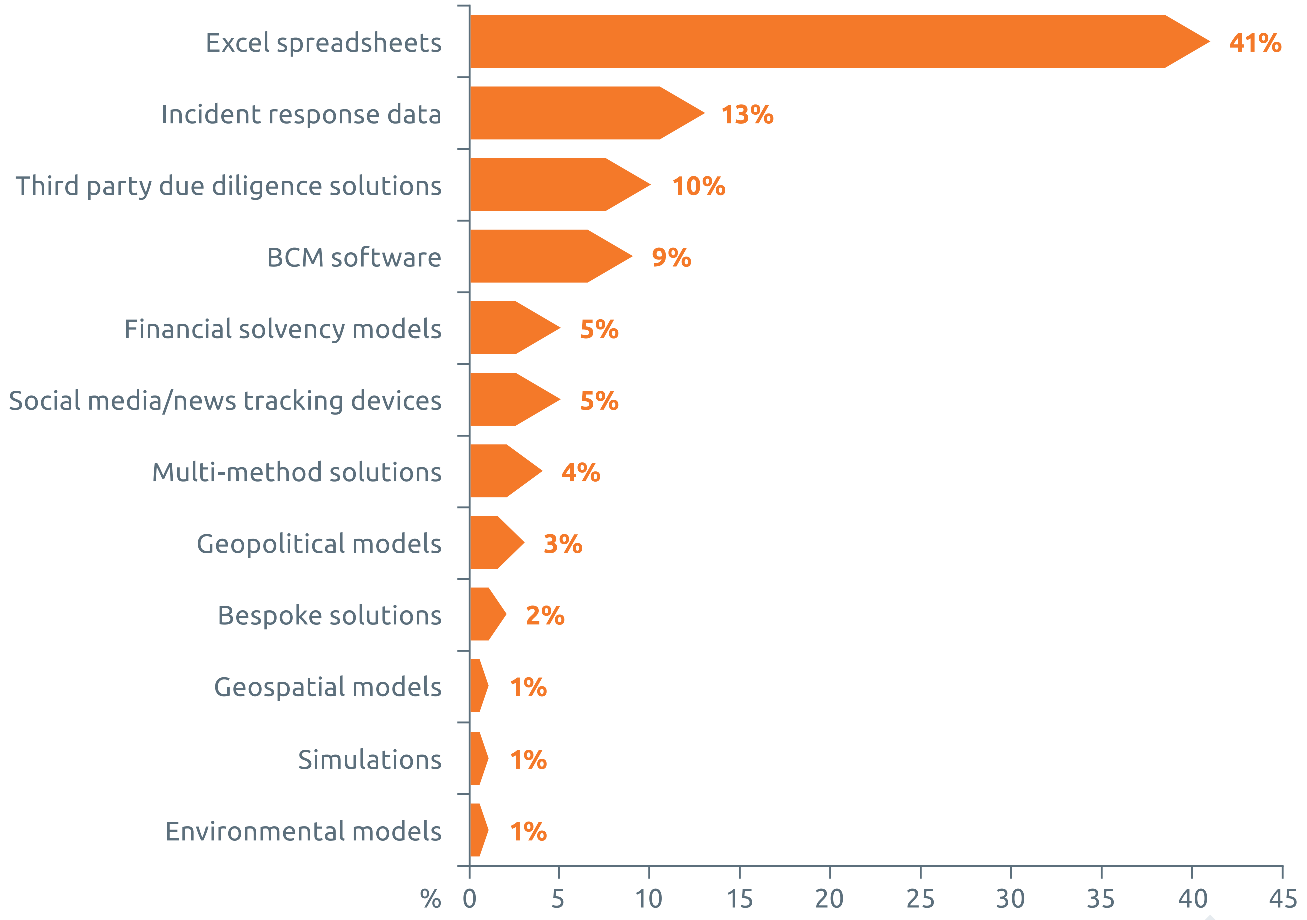


Fig 3: Question 8. What types of solutions do you rely on to analyse, track or monitor potential issues causing supply chain disruptions? (Please indicate all that apply - figures might exceed 100%; N=159)

The number of professionals reporting more than 20 disruptions has reduced by 10% (from 13% to 3%) compared to last year (Figure 4). However, the majority of organizations (65%) have experienced at least one disruption in the past year.

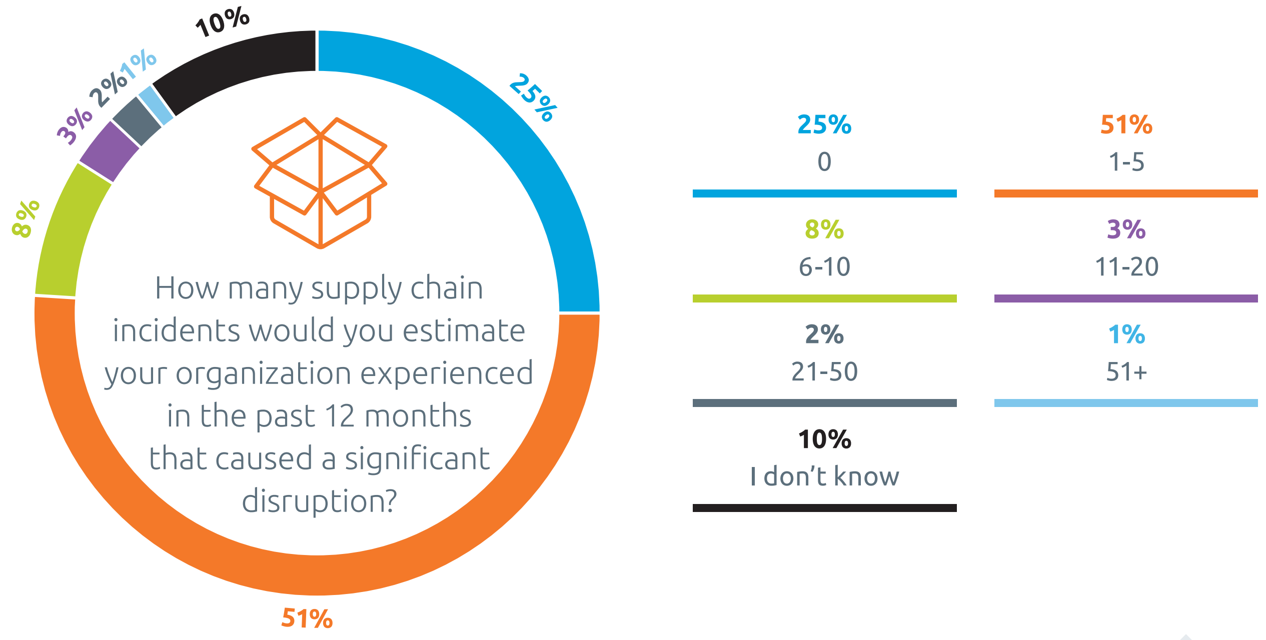


Fig. 4: Question 9. How many supply chain incidents would you estimate your organization experienced in the past 12 months that caused a significant disruption? (N=361)

[1] forbes.com/sites/bernardmarr/2016/04/22/how-big-data-and-analytics-are-transforming-supply-chain-management/#2f991a7d39ad

Respondents comment on specific instances of **supply chain disruption.**

"There are robust contracts and contingency plans in place to prevent the majority of disruptions from causing significant issues."

"A major power outage at a supplier's data centre caused an incident. However, the solution was geo-resilient and it did not affect the business."

"A black out of our internet service provider caused a significant disruption. We had a solid alternative that avoided losing time and money; however, the essential services are still very vulnerable and not regulated enough."

"Our supplier was not up to the task and since we had a long-term contract with them we mutually agreed to terminate the contract and switch to another supplier to complete the programme and cover the years left in the original contract term."

"A major earthquake occurred in the Kumamoto area which caused transportation and shipping to that area to be stopped, causing a disruption."

"The majority of the supply chain disruptions relate to one upstream supplier (we work in a monopoly market so there is no alternative supplier), causing additional operational costs for our organization. These disruptions are accepted by the supplier and present several challenges, largely due to differences in risk appetite and risk tolerance between the two organizations."

Nearly half of the respondents (44%) report Tier 1 suppliers as the predominant source of disruption, with almost an additional quarter (24%) stating disruptions mainly come from Tier 2 (Figure 5). On a positive note, the number of organizations that do not analyse the source of disruption to their supply chain has decreased from 40% to 22% compared to last year.

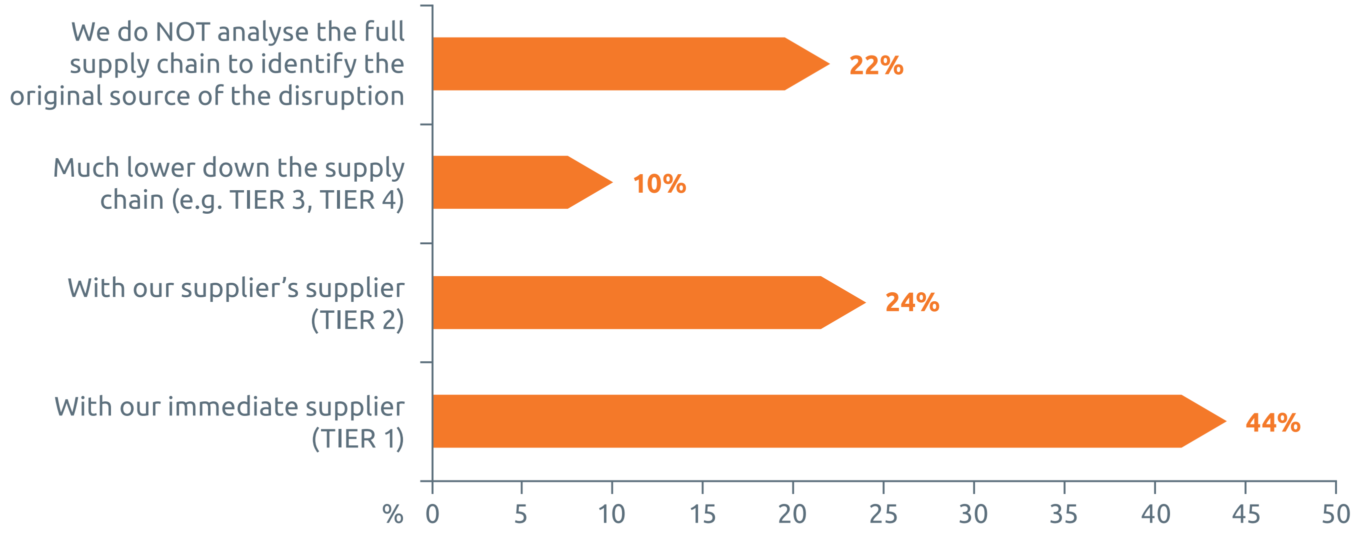


Fig. 5: Question 10. Considering the supply chain incidents you are aware of in the last 12 months, which of the following apply in your experience? The predominant source of disruption across all events was: (N=301)

Causes of disruption

Unplanned IT or telecommunications outages (48%) are still the main cause of disruption, with cyber attacks and data breaches and loss of talent/skills completing the top three (Figure 6). Interestingly, outsourcer failure (33%) moves up from fifth to fourth place this year, followed by transport network disruption (26%). Further down, adverse weather remains in sixth position, among increasing concerns about climate change, while fire jumps up to number seven from number fourteen last year. New laws and regulations, insolvency in the supply chain, and energy scarcity round up the top ten. Act of terrorism slides down compared to last year's 9th place, but only to be found in 11th place, confirming this is still a considerable threat for organizations. Segmenting the data per geographical region, it is worth noting that Australasia seems to be more affected by weather hazards, as respondents from this region feature adverse weather as the main cause of disruption (46%) and earthquake/tsunami ranked third (33%).

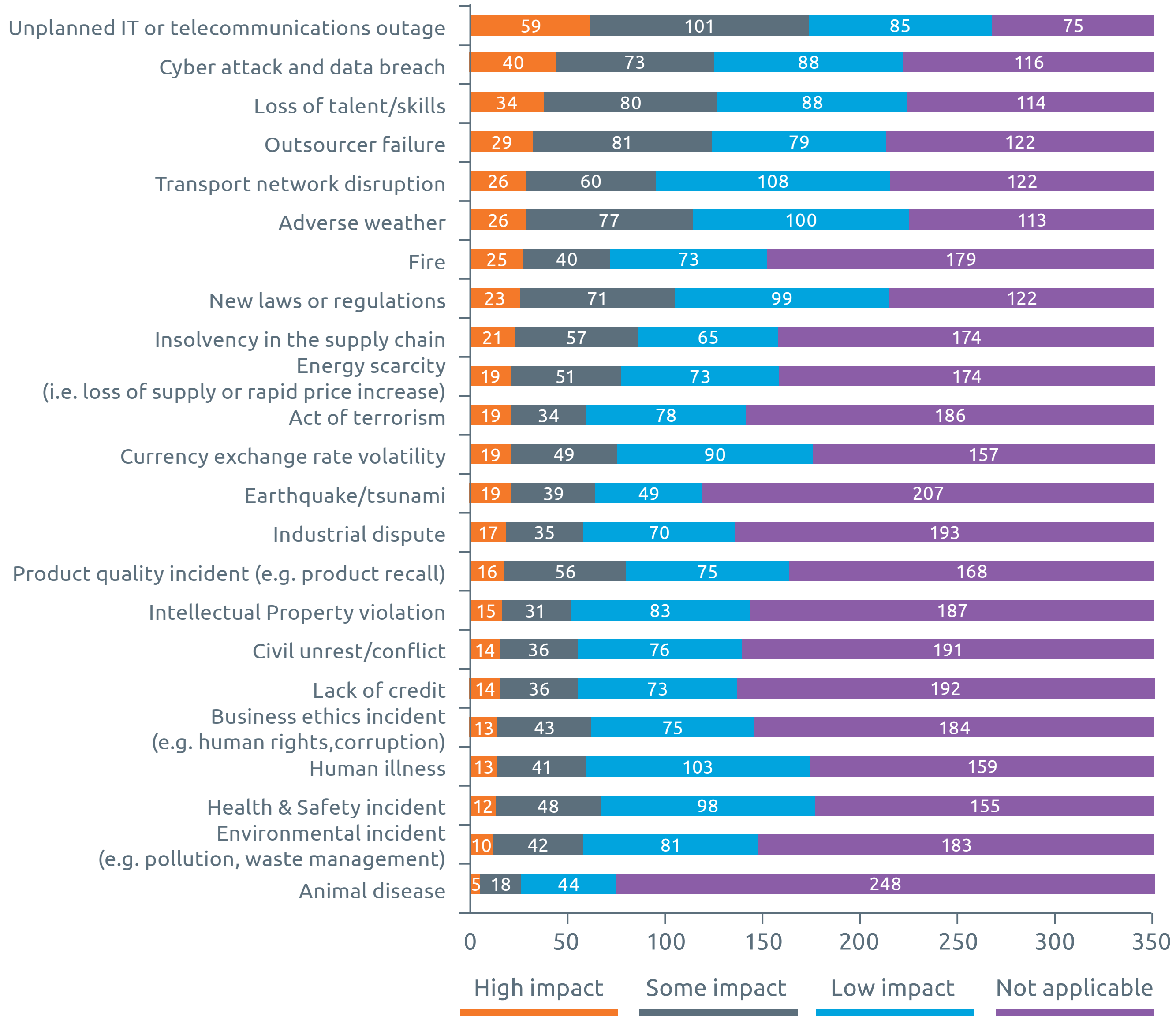


Fig. 6: Question 11. How severely has your supply chain been affected by any of the following sources of disruption over the past 12 months? (Please tick all that apply - figures might exceed 100%; N=330)

Consequences of disruption

Loss of productivity (55%), increased cost of working (46%), and customer complaints (43%) remain as the top three impacts of supply chain disruptions (Figure 7). As the graph allows for multiple responses, it is interesting to consider how organizations might have suffered multiple consequences following a single incident. For instance, the loss of productivity might lead to loss of revenue (32%), or customer complaints might be connected to damage to brand reputation (31%).

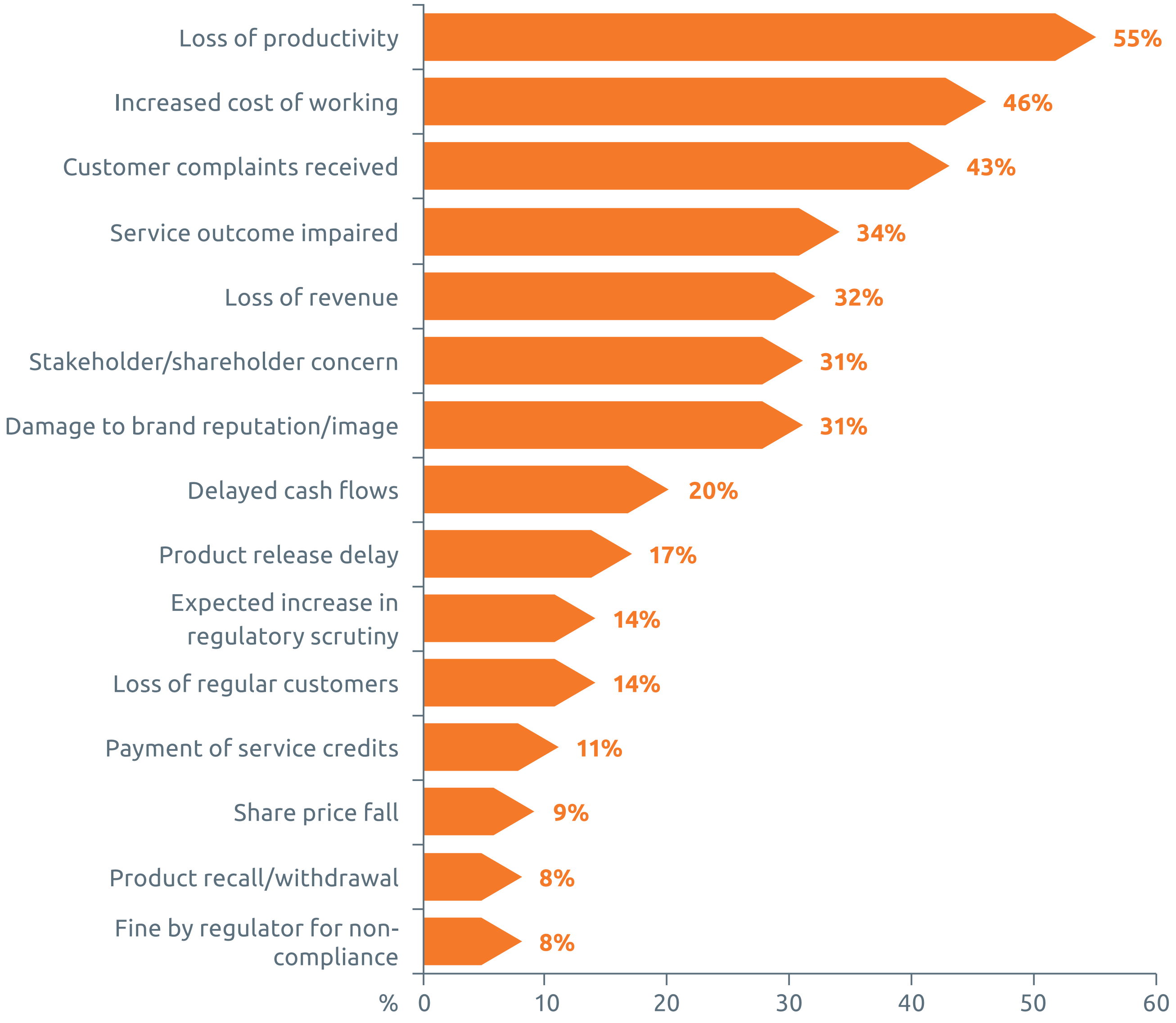
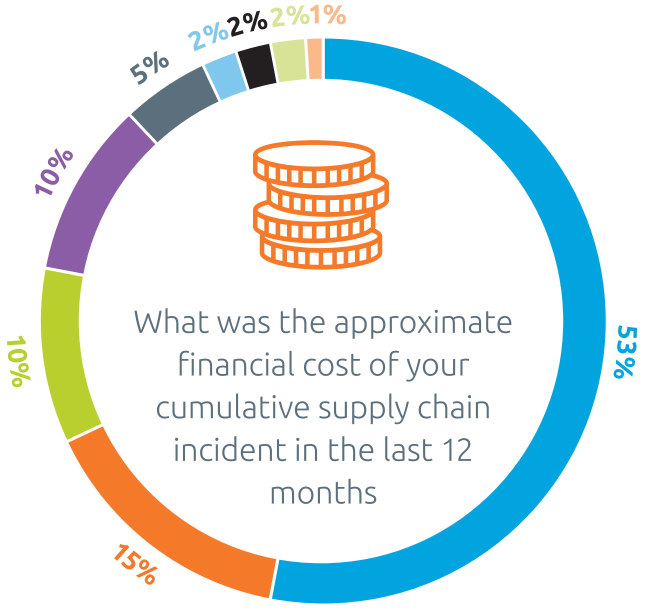


Fig 7: Question 12. Which of the following impacts or consequences arose from the incidents/disruptions experienced in the last 12 months? Tick as many as applicable. (Please tick all that apply - figures might exceed 100%; N=265)

Economic impacts of disruption

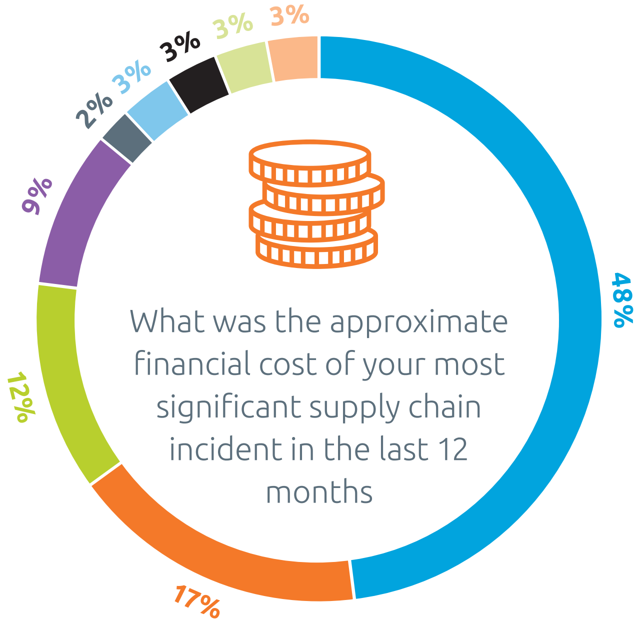
More respondents this year (53%) tend to report losses for less than 50,000 euros compared to last year (33%). Similarly, losses of more than one million euros decrease from 34% to 22% (Figure 8). Less costly incidents could be due to an increasing uptake of business continuity arrangements over the years as well as an increase in top management commitment[2].



53% Less than €50,000	**15%** €50,001-250,000
10% €250,001-500,000	**10%** €1-10 million
5% €11-50 million	**2%** €51-100 million
2% €101-250 million	**2%** €251-500 million
1% Greater than €500 million	

Fig. 8: Question 13.1. What was the approximate financial cost of your cumulative supply chain incident in the last 12 months (loss of revenue and/or increased cost of working)? (N=205)

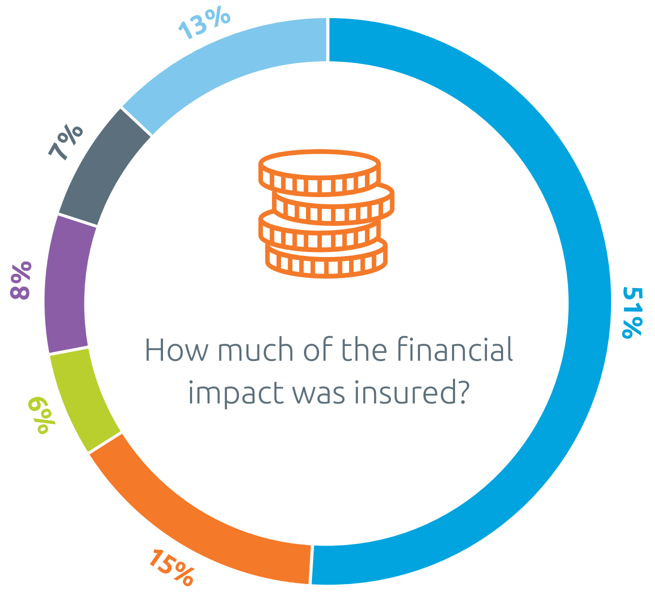
Nonetheless, looking at single incidents affecting the supply chain it is worth noting that disruptions costing more than 1 million euros have increased from 9% to 23% (Figure 9).



48% Less than €50,000	**17%** €50,001-250,000
12% €250,001-500,000	**9%** €1-10 million
2% €11-50 million	**3%** €51-100 million
3% €101-250 million	**3%** €251-500 million
3% Greater than €500 million	

Fig. 9: Question 13.2. What was the approximate financial cost of your most significant supply chain incident in the last 12 months (loss of revenue and/or increased cost of working)? (N=148)

The majority of respondents (51%) report their losses were not insured, a negative trend compared to last year's 43% (Figure 10). On the other hand, the number of organizations fully insuring their losses has grown from 4% to 13%, while those insuring more than 50% of their losses has grown from 20% to 28%. These figures reveal mixed results, meaning that while there has been some progress there is still work to do in order to build resilient supply chains.



51% 0%, losses were uninsured	**15%** 1-25%
6% 26-50%	**8%** 51-75%
7% 76-99%	**13%** 100%, losses were fully insured

Fig. 10: Question 14. How much of the financial impact was insured? (N=175)

[2] See figure 12&13

Respondents share their other experiences of **supply chain disruption.**

"The financial impact is complete guesswork. A majority would have been insured."

"A supplier for surgical implants made quite a number of defective implants. This resulted in some surgical procedures being suspended. The company is currently in negotiation with a new supplier and some patients are being referred to competitors."

"In the last 10 years, the most serious disruptions were caused by energy providers, central payment infrastructure, and telecom/ data providers. "

"Our organization is often affected by short power outages, but we have a UPS that covers disruptions up to 1 hour. In case of longer outages, we tend to work from home."

"Our 'very high impact' HS&E incident is still under investigation. It caused a site to be decommissioned by a third party and it resulted in fatalities - this has potential to be a single significant loss."

Horizon scanning supply chain threats

Consistent with the causes of disruption highlighted previously in this report, respondents consider cyber attacks and data breaches (60%), unplanned IT or telecommunications outage (59%) and loss of talent /skills (34%) as their main concerns for the next 12 months (Figure 11). Interestingly, act of terrorism (21%), product quality incident (20%) and health & safety incident (20%) feature in the top ten, even if they were not listed as main causes of past disruptions.

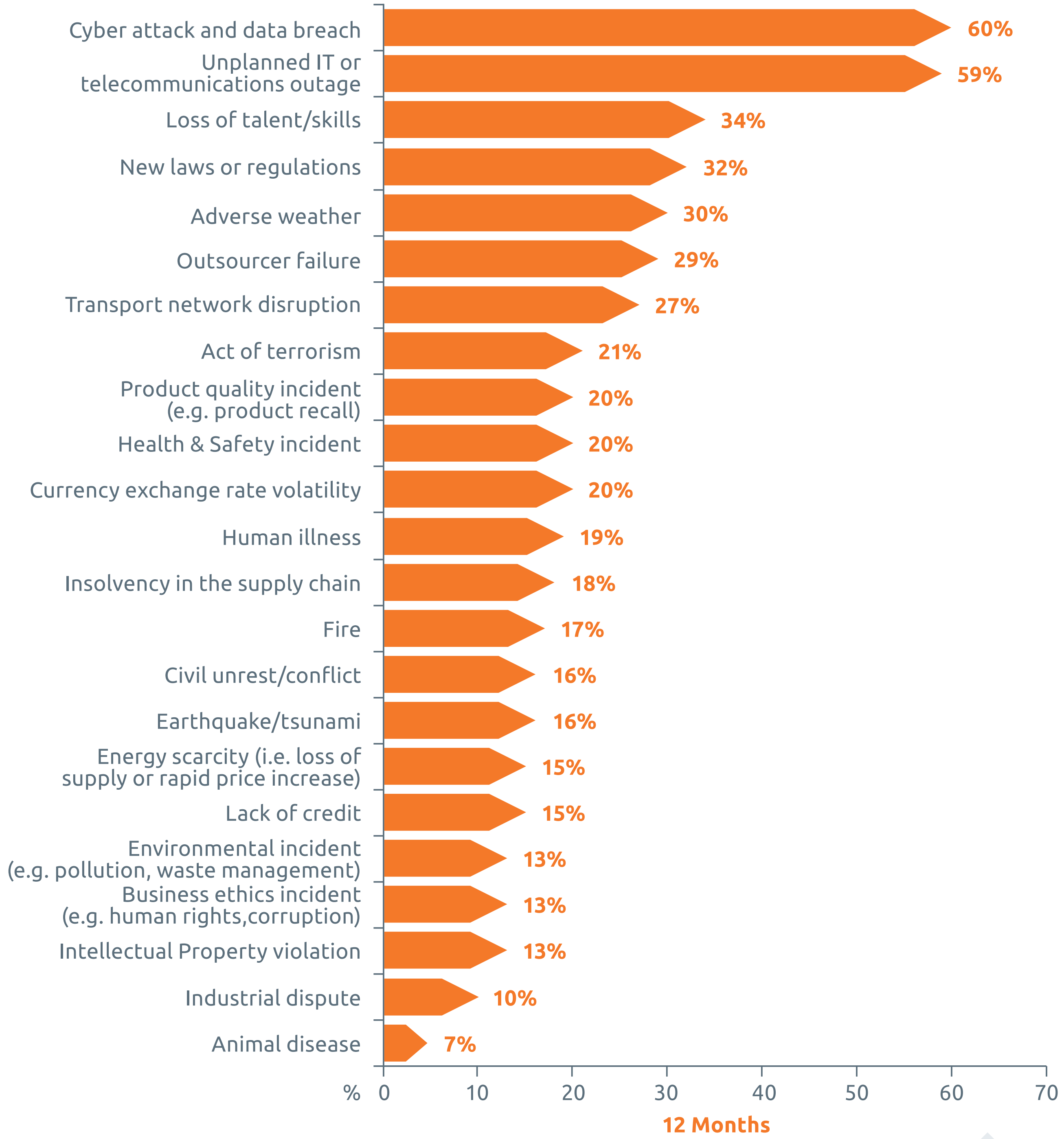


Fig. 11: Question 16.1. Looking ahead, what do you see as the biggest risk(s) to your supply chain? Tick as many as applicable. (Please tick all that apply - figures might exceed 100%; N=282)

Concerns over the next five years somewhat differ. While cyber attacks and data breaches (48%) remain on top of the chart, at number two (40%) new laws or regulations jump up by two places (Figure 12). This could be due to the introduction of new pieces of legislation such as the upcoming General Data Protection Regulation (GDPR) in Europe that will enter into force in 2018. It is also worth mentioning that both adverse weather (29%) and earthquake/tsunami (24%) make it to the top ten, showing growing concerns towards extreme weather events and natural disasters.

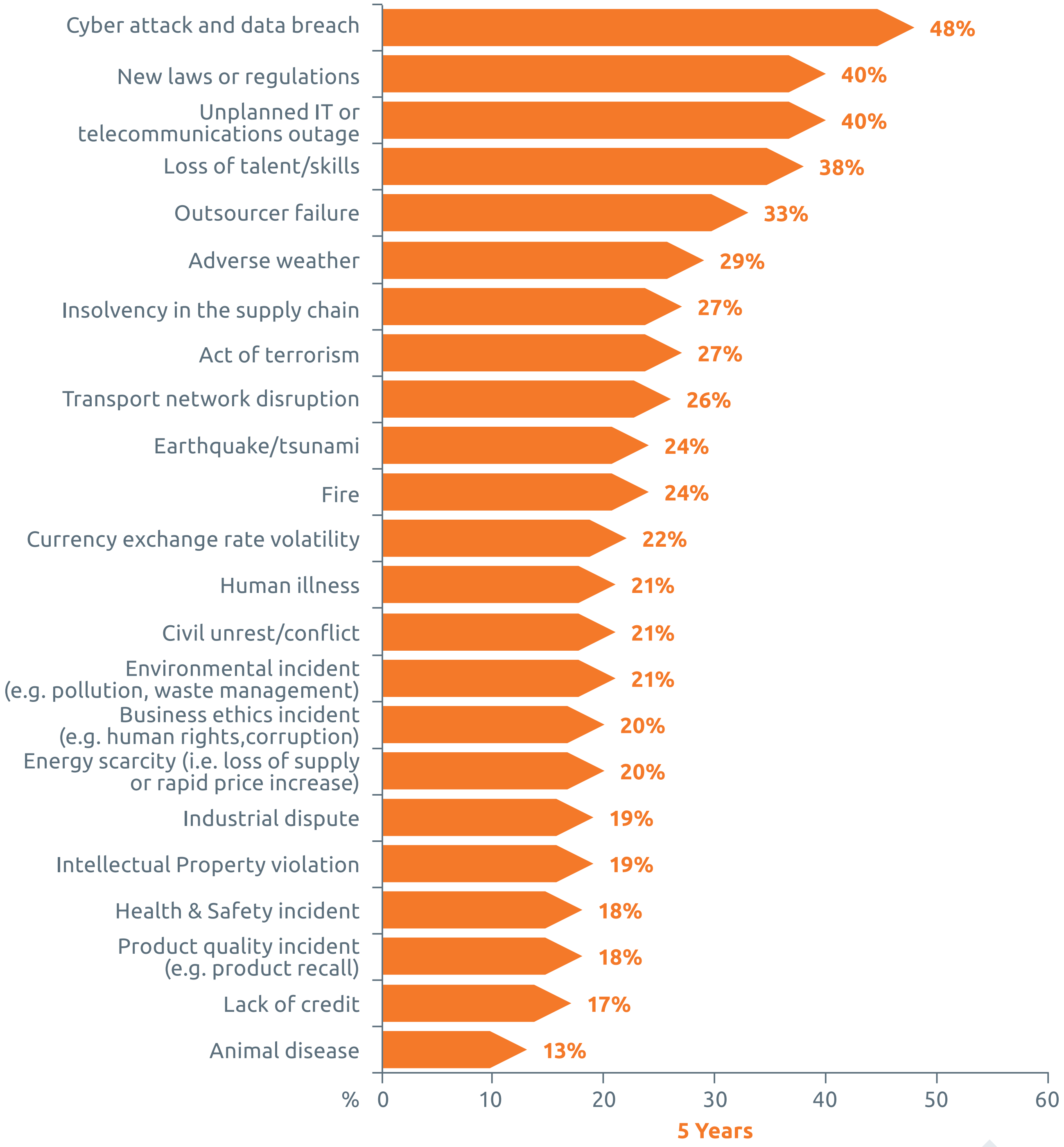


Fig. 12: Question 16.2. Looking ahead, what do you see as the biggest risk(s) to your supply chain? Tick as many as applicable. (Please tick all that apply - figures might exceed 100%; N=282)

An expert weighs in

Matthew Hillyer

Understanding cyber risk within the supply chain

The cyber risk presented within our supply chains is a rapidly growing area of concern for Cyber Risk Management professionals. It is therefore extremely important to be able to identify and mitigate cyber risks which arise from our desire to increase collaboration, allow system connectivity and enhance the ease and speed of doing business with our network of suppliers.

To assess the quality of our suppliers in their management of data and ultimately their vulnerability to cyber-attack, we need to review and understand their processes and procedures across seven critical risk indicators:

1. Leadership and Management

a. Does the leadership team recognise and manage Cyber as a strategic risk?

b. Do the senior leaders within the organization buy into and champion the cyber risk programmes being deployed?

2. Strategy and Policy

a. Are policies up to date and refreshed to reflect new risks and ways of working?

b. Have the strategies and policies been communicated at all levels and can it be demonstrated that people understand them?

3. People and Training

a. Is there regular cyber risk training with the content refreshed to reflect current trends or emerging threats?

b. Has the organization established clear roles or objectives for managing information risk, not just focused on an Information Security Manager?

4. IT and Infrastructure

a. Is computer hardware managed so that patches are installed quickly when they become available?

b. Do controls around emails help prevent data leakage through the use of data classification and encryption?

5. Supply Chain

a. Do they have established information sharing protocols?

b. Do they employ a similar rigour to yourselves in assessing the performance of their suppliers in respect to data management?

6. Incident Management

a. Does the organization have a clear process for identifying a breach and a process for reporting it?

b. Does the organization have a specific Business Continuity Plan for Cyber or have they tested their current plans for their suitability to respond to a cyber-attack?

7. Compliance and Governance

a. Is there a culture of continuous improvement within the organization?

b. Does the audit plan test the Information Security controls?

We can never truly close off our network perimeters to our supply chain as this is business limiting. We can however, through the identification and prioritisation of the suppliers which have the best information security procedures and engender the right culture to approach and manage cyber risk, create a supply chain which is focused on developing and enhancing its cyber resilience.

About the Contributor:

Matthew Hillyer is Senior Strategic Risk Consultant at Zurich. He is an experienced risk management professional with a background in implementing enterprise risk management and growing organizational risk maturity. He is a contributor to the Institute for Risk Management's guidance paper on Cyber Risk. In 2012 he was awarded the CIR Magazine Risk Manager of the Year award.

3 Supply Chain Resilience and Business Continuity

Top management commitment

Top management commitment has been consistently identified in this study as a key driver of supply chain resilience. The presence of management buy in and leadership are crucial to encouraging good practice that enables greater supply chain resilience. The increase in top management commitment reported by organizations in this year's report from 27% to 41% is therefore seen as welcome news (Figure 13). In segmenting the data, high top management commitment is observed to be greater in large organizations than in small and medium-sized enterprises (SMEs) at 44% compared to 33%.

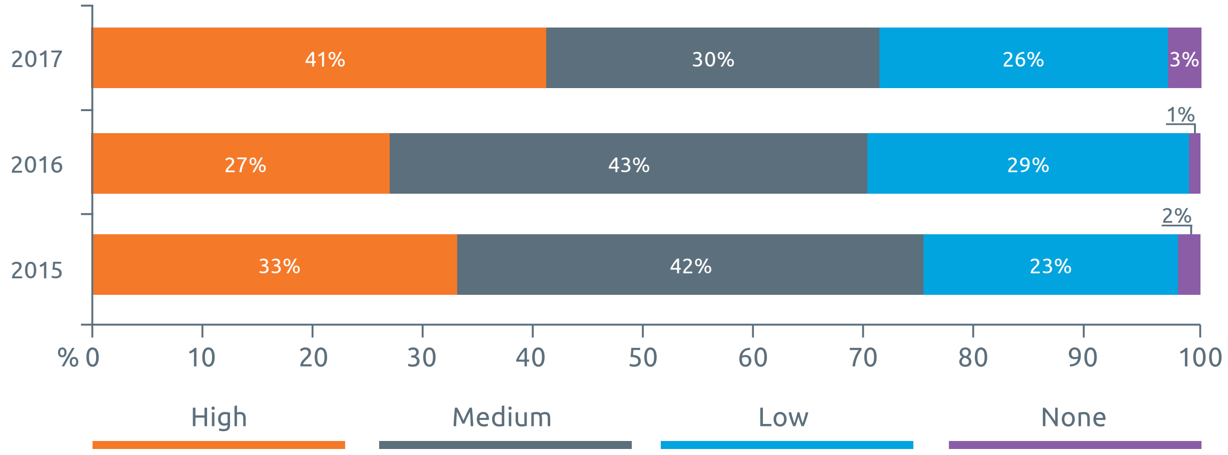


Figure 13: Question 17. How would you assess your organization's top management commitment to managing supply chain risk? (N=261)

High top management commitment is also observed to coincide with greater supply chain visibility overall. Organizations who report high top management commitment are almost four times more likely to have firm-wide reporting than those organizations who responded with 'low' or 'none' (45% to 12%). This gap has more or less widened compared to last year's results (55% to 19%). This result emphasises how top management commitment is essential to encouraging good practice which improves supply chain resilience.

Business continuity arrangements

Almost three-quarters of organizations (74%) report having business continuity arrangements related to supply chain management (Figure 14). This is more or less consistent with last year's results. Results over the last five years also demonstrate the relatively widespread uptake of business continuity (Table 2).

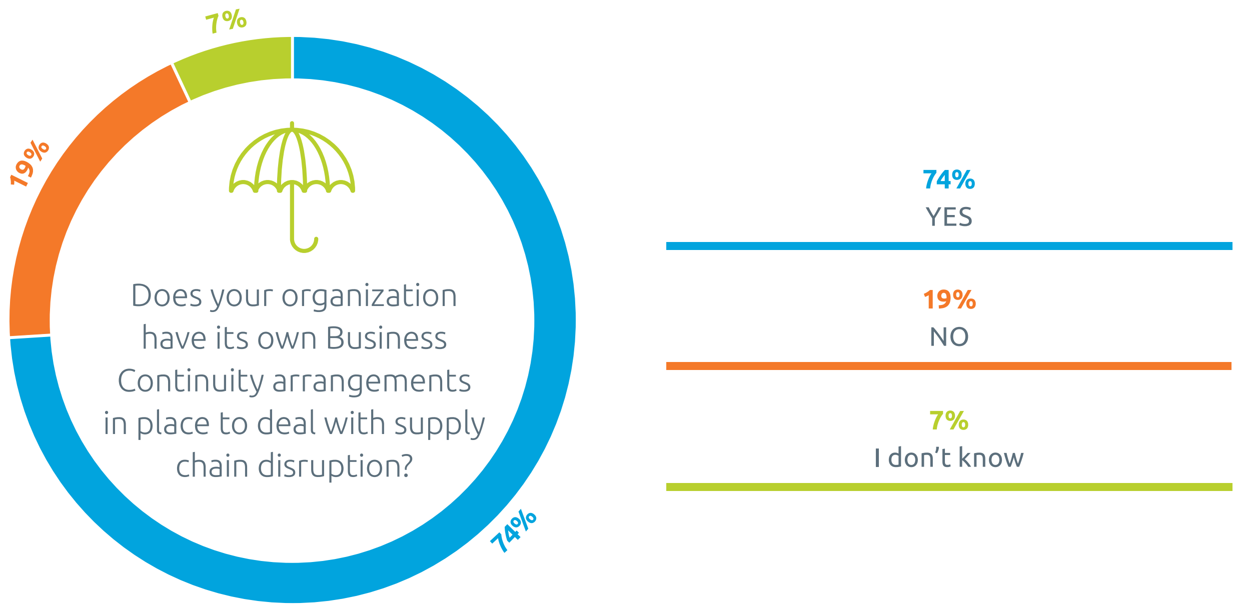


Figure 14: Question 18. Does your organization have its own Business Continuity arrangements in place to deal with supply chain disruption? (N=297)

Year	Yes	No	Don't know	N
2013	75%	19%	6%	405
2014	72%	22%	6%	375
2015	68%	25%	7%	323
2016	73%	25%	7%	358
2017	74%	16%	10%	285

Table 2. Tracking supply chain business continuity arrangements, 2012-2017

The presence of clear business continuity arrangements is seen to reinforce good practice. Organizations having such arrangements are eight times more likely to report greater supply chain visibility. They are also almost twice more likely to insure for supply chain losses and three times more likely to display top management commitment essential to reinforcing good practice (Table 3).

Indicator	Business continuity arrangements present (Q18)	No business continuity arrangements (Q18)
Firm-wide reporting of supply chain disruption (Q6)	41%	5%
Insuring for supply chain losses (Q14)	54%	29%
High top management commitment to supply chain resilience (Q17)	49%	15%

Table 3. Comparing practices between organizations with or without supply chain business continuity arrangements

Large organizations again outperform SMEs in terms of having business continuity arrangements related to supply chains (Figure 15). Large organizations also outpace SMEs in indicators associated with good practice except on firm-wide reporting of disruption, on which they seem to be quite even (Table 4).

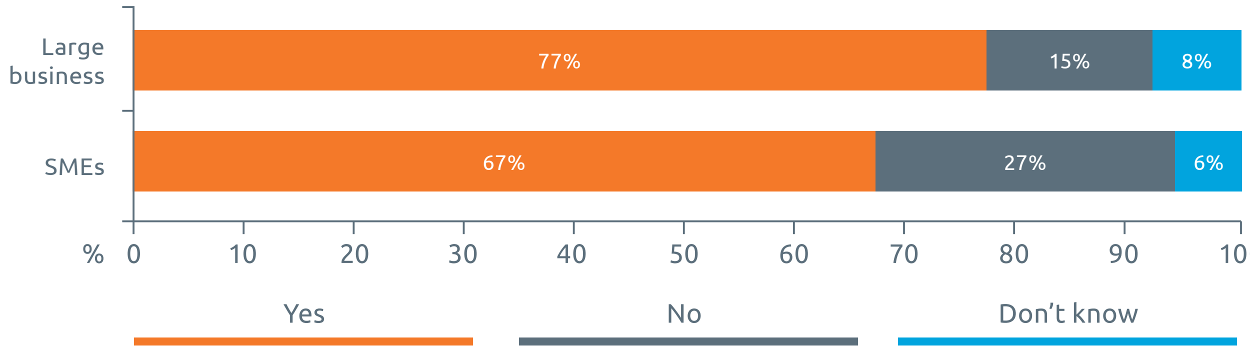


Figure 15: Question 18. Does your organization have its own Business Continuity arrangements in place to deal with supply chain disruption? (N=297)

Indicator	SMEs	Large businesses
Firm-wide reporting of supply chain disruption (Q6)	31%	32%
Insuring for supply chain losses (Q14)	40%	55%
High top management commitment to supply chain resilience (Q17)	33%	44%

Table 4. Comparing practices between SMEs and large businesses

Supplier business continuity information

The immense complexity of global supply chains is a consistent finding in this report and this year's figures affirm this. Almost four out of 10 organizations (38%) report having 21 or more key suppliers. Meanwhile, 2% claim having more than 1,000 key suppliers. The percentage of organizations who do not identify key suppliers has dropped from 14% to 7% (Figure 16).

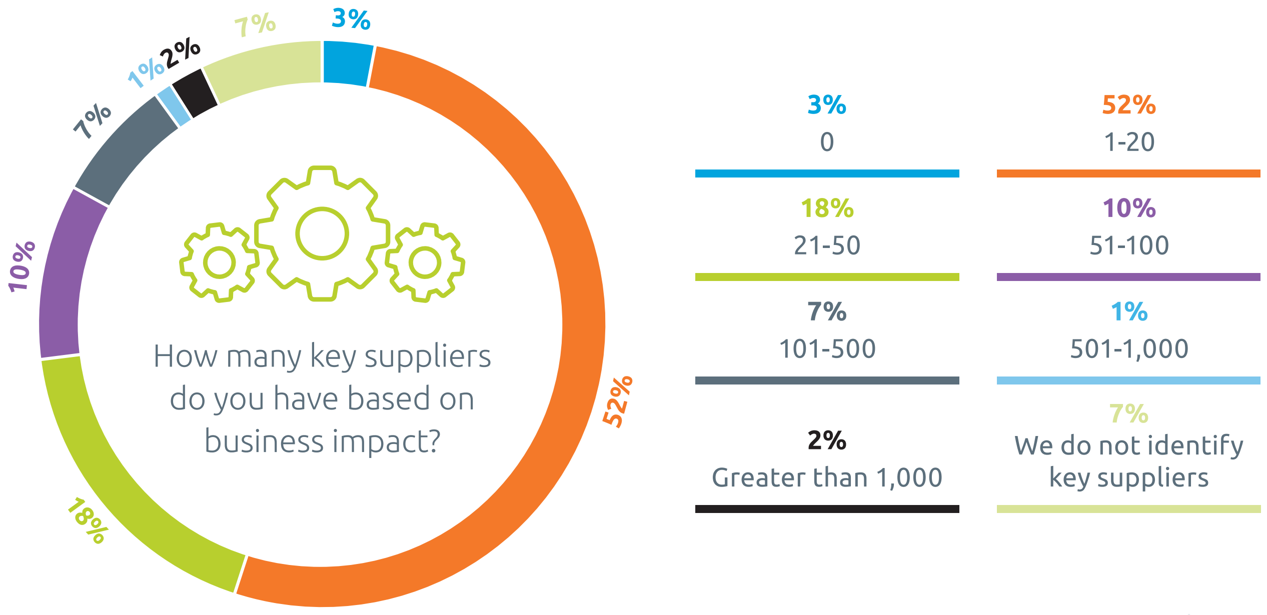


Figure 16: Question 19. How many key suppliers do you have based on business impact? (N=297)

Among other behaviours, identifying key suppliers is a good indicator of good practice which improves supply chain resilience (Table 5). Business continuity practitioners can collaborate with their supply chain counterparts in assessing suppliers based on their business impact and work out relevant arrangements which could improve recovery from supply chain incidents.

Indicator	Identifying suppliers (Q19)	NOT identifying key suppliers (Q19)
Firm-wide reporting of supply chain disruption (Q6)	33%	11%
Insuring for supply chain losses (Q14)	49%	25%
High top management commitment to supply chain resilience (Q17)	41%	29%

Table 5. Comparing practices between organizations as to identification of key suppliers

Almost three quarters of organizations (74%) ask their key suppliers (new and existing) about their business continuity arrangements, a considerable increase from last year's 63% (Figure 17). Once more, this behaviour coincides with other areas of good practice, especially with firm-wide reporting of disruption which increases supply chain visibility (Table 6).

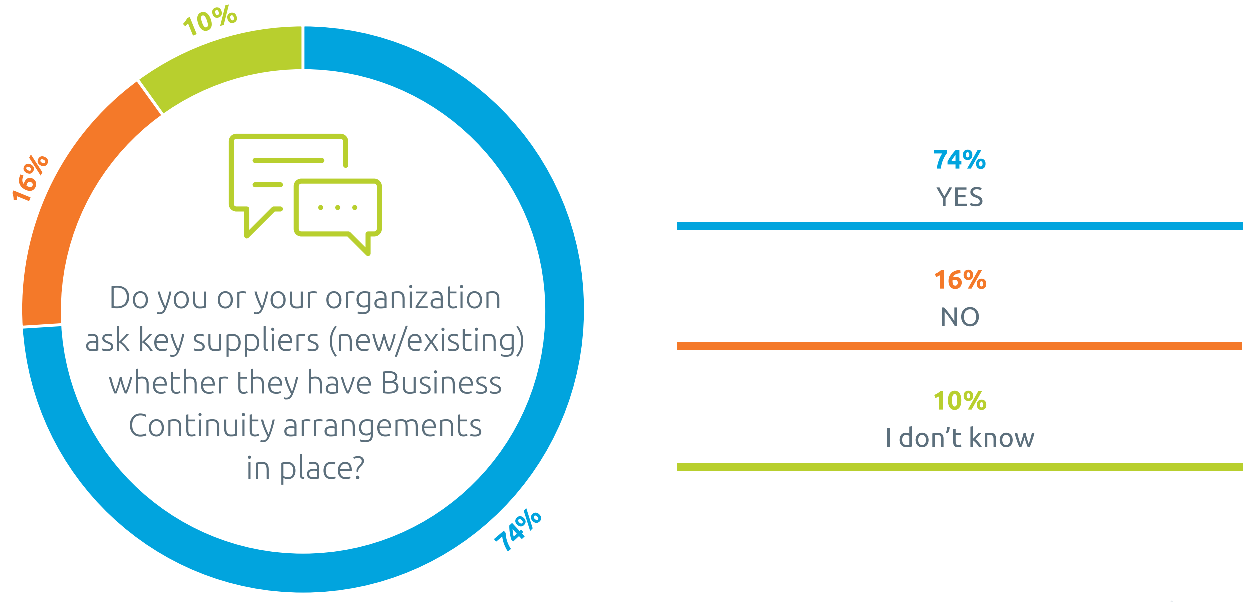


Figure 17: Question 20. Do you or your organization ask key suppliers (new/existing) whether they have Business Continuity arrangements in place? (N=285)

Indicator	Asking key suppliers about business continuity arrangements (Q20)	NOT asking key suppliers about business continuity arrangements (Q20)
Firm-wide reporting of supply chain disruption (Q6)	39%	9%
Insuring for supply chain losses (Q14)	51%	36%
High top management commitment to supply chain resilience (Q17)	44%	17%

Table 6. Comparing practices between organizations as to asking key suppliers about business continuity arrangements

Less than half of organizations (47%) claim that the majority of their suppliers have business continuity arrangements, a figure unchanged from last year's. Less than 10% of organizations report that all of their suppliers have business continuity in place (Figure 18). As business continuity is an essential contributor to overall supply chain resilience, these figures pose a challenge for business continuity practitioners to engage with their supply chain management and procurement counterparts in drawing up policies or contractual arrangements with suppliers. Given that the presence of business continuity coincides with other areas of good practice associated with improved supply chain management, it can be used as a way to 'sell' the importance of business continuity and its link to overall resilience.

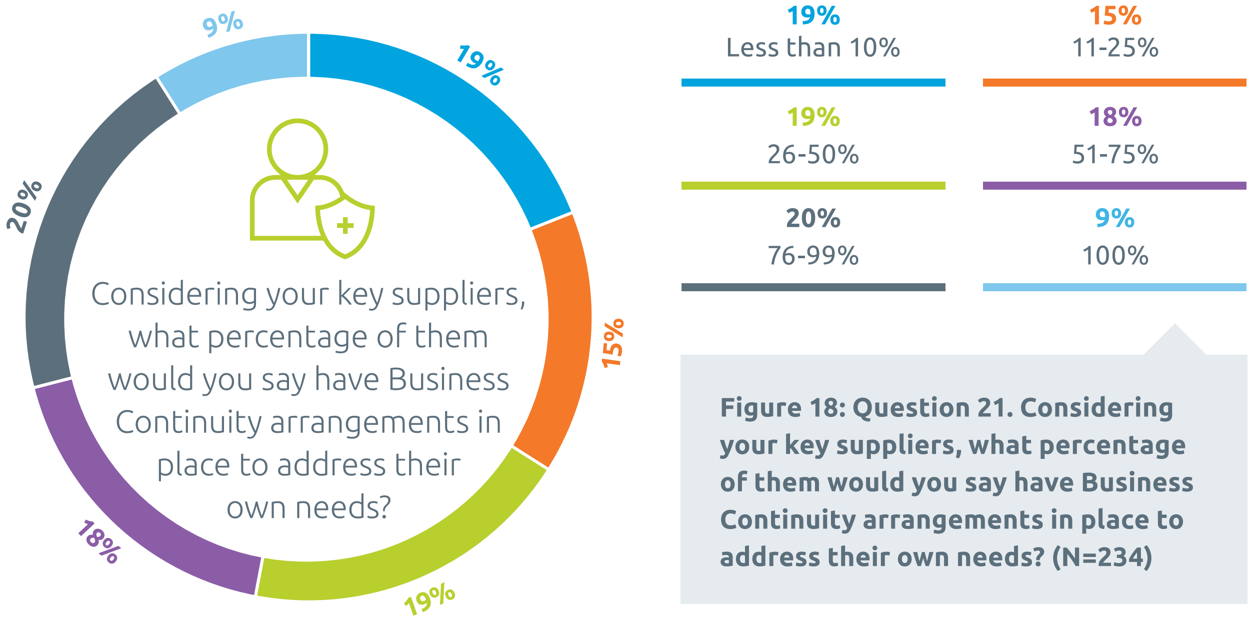


Figure 18: Question 21. Considering your key suppliers, what percentage of them would you say have Business Continuity arrangements in place to address their own needs? (N=234)

Seeking assurance from key suppliers

Seeking assurance from key suppliers is another important area of engagement between business continuity practitioners and their supply chain and procurement counterparts. This year's results affirm the growing importance of relevant industry standards and the role of business continuity in assurance.

The percentage of organizations requiring alignment (46% to 50%) or certification (32% to 40%) against industry standards have considerably increased this year. More organizations are also observed to check the scope of the business continuity management (BCM) programmes of their key suppliers (34% to 40%). This is complemented by the increasing demand for compliance to good practice such as those contained in the BCI Good Practice Guidelines (35% to 42%) (Figure 19).

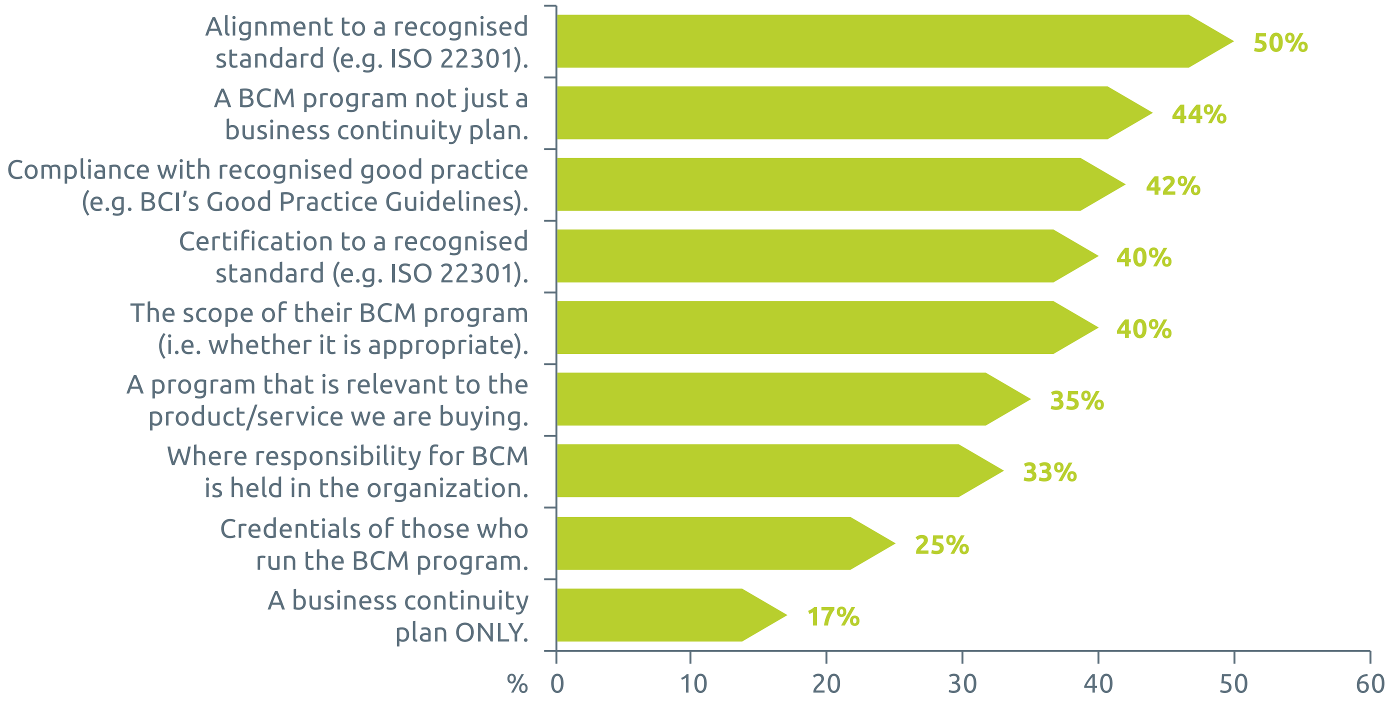


Figure 19: Question 22. What information do you seek in order to better understand the Business Continuity arrangements of key suppliers? (Please tick all that apply - figures might exceed 100%; N=263)

There are a variety of ways that organizations obtain this assurance. Administering self-assessment questionnaires remains a popular way of obtaining assurance, followed by requiring copies of supplier documentation. It is also interesting to note that the percentage of organizations not collecting any information has dropped from 25% in 2016 to 14% this year (Figure 20).

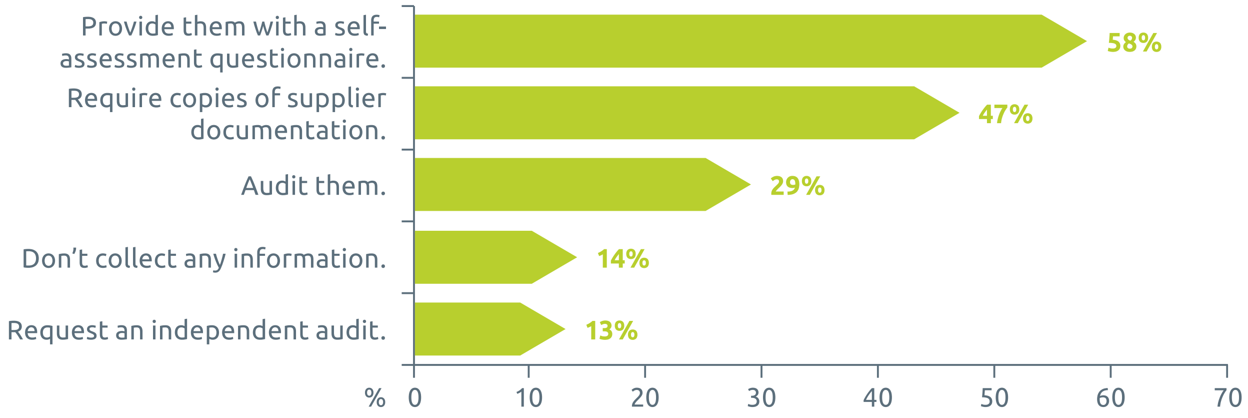


Figure 20: Question 23. How do you collect this information? We…
(Please tick all that apply - figures might exceed 100%; N=271)

Respondents share their experiences in seeking assurance from their **key suppliers**

"Our contracts have legal clauses providing for audits or inspections of suppliers. There is a requirement for vendors to have a business continuity programme and conduct joint testing with our organization."

"We ask for test results of their business continuity plans (BCP) and disaster recovery plans (DRP)."

"The standard for us is the provision of a Business Continuity Management (BCM) Statement in the Service Level Agreement, requesting leading certifications and claiming the 'Right to Audit' for critical suppliers who are not monopolists or central institutions."

"We also request information on their recovery capability and location of manufacturing, which enables us to assess location risks."

"We reserve the right to audit insufficient responses [to our supplier questionnaire]."

"The presence of contingency plans is required for the contract bidding process."

Assessing effectiveness of supplier business continuity

Validating supplier business continuity is another key area of engagement among business continuity and supply chain practitioners. As more organizations require business continuity management and similar assurance as a pre-requisite to bidding and procurement, it is essential that relevant personnel validate these. Previous editions of the report have raised the absence of validation as an enduring challenge for many organizations. This remains the case as 47% of organizations do not check suppliers' business continuity arrangements (Figure 21). Nonetheless, this has dropped considerably from 57% in 2016 and 56% in 2015, which suggests changes in many organizations are afoot.

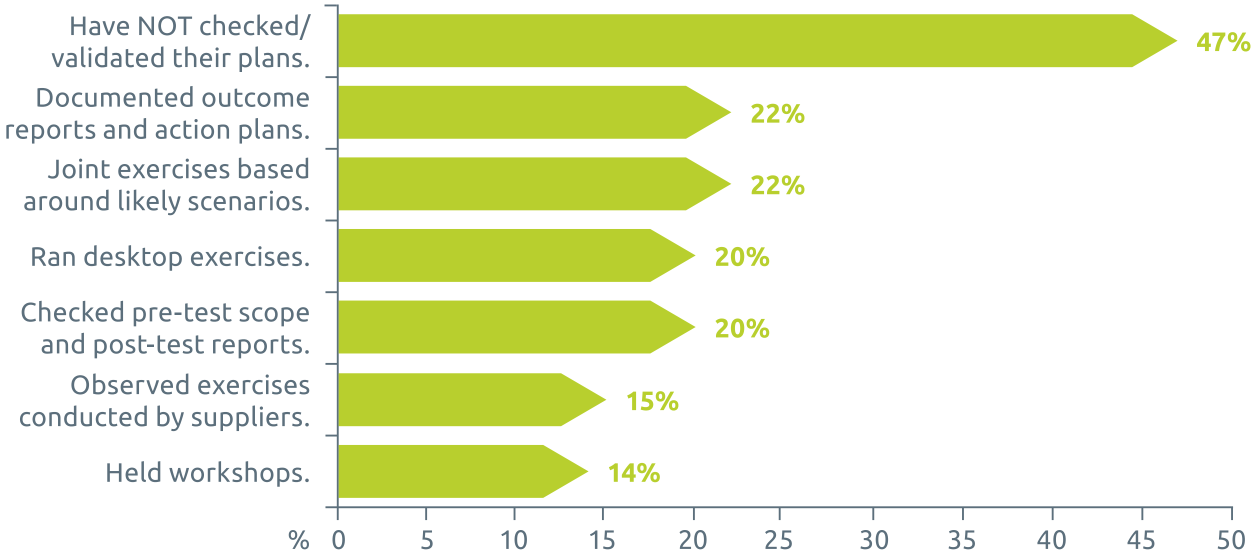


Figure 21: Question 24. How have you checked/validated that key suppliers' Business Continuity arrangements might work in practice? (Please tick all that apply - figures might exceed 100%; N=268)

More than a third of organizations (36%) conduct scheduled review meetings with their suppliers, an increase from 30% last year. The percentage of organizations who never review suppliers' business continuity arrangements has also dropped slightly from 16% to 13% (Figure 22).

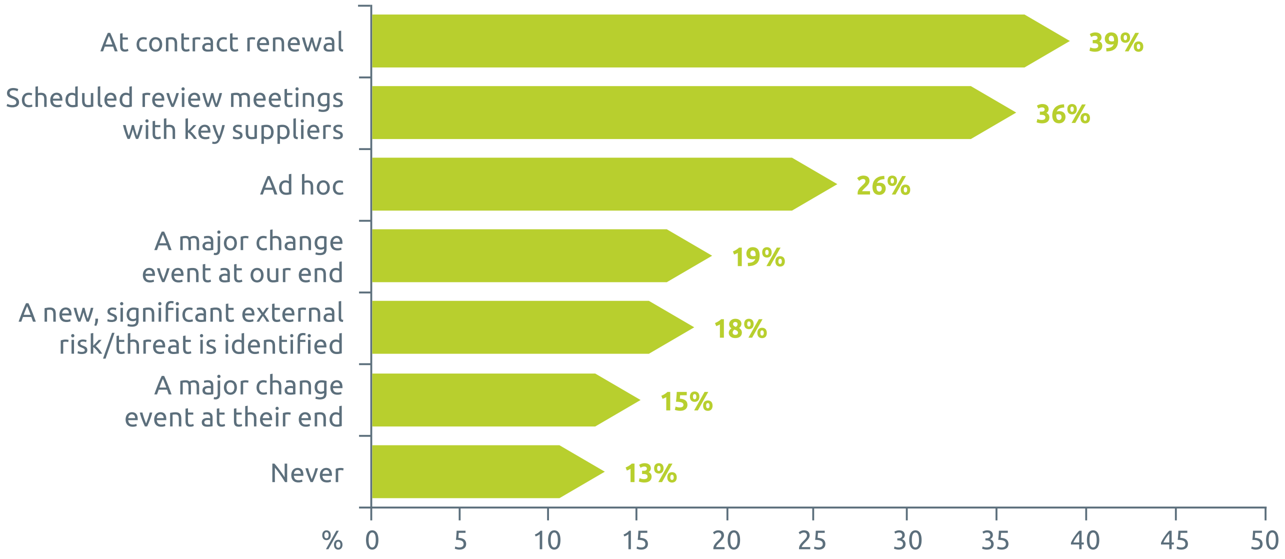
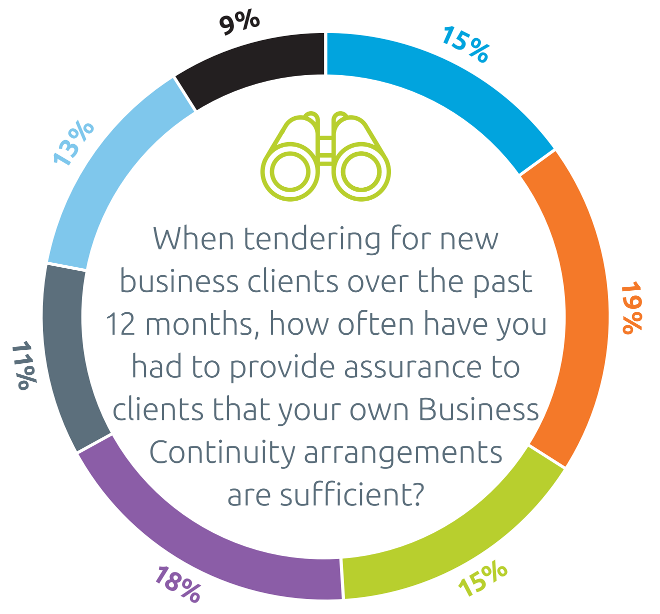


Figure 22: Question 25. How often do you review your Business Continuity requirements with key suppliers and their capability to meet them? (Please tick all that apply - figures might exceed 100%; N=266)

There also seems to be a growing uptake among clients in terms of requiring business continuity arrangements as a pre-requisite for tender. The percentage of organizations who provide client assurance through business continuity arrangements in every tender has risen substantially from 6% to 15% (Figure 23).



15%
Every tender/ proposal (100%)

19%
Majority (51-99%)

15%
Sometimes (25-50%)

18%
Rarely (1-24%)

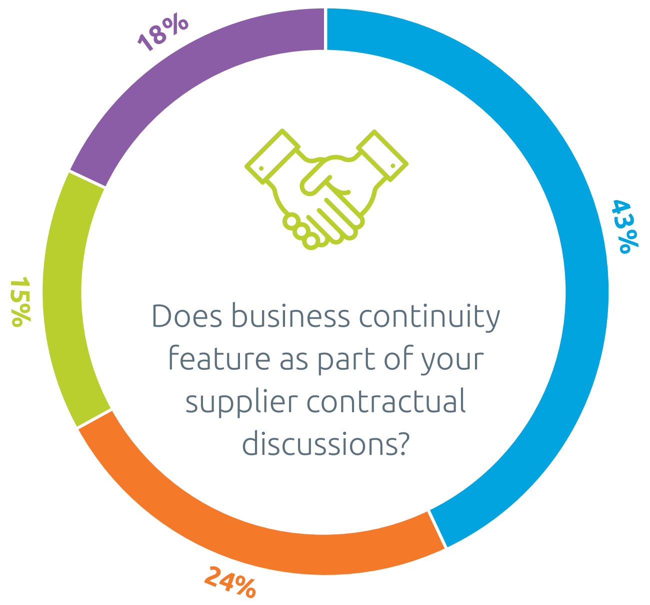
11%
Not at all (0%)

13%
Don't know

9%
Not applicable

Figure 23: Question 26. When tendering for new business clients over the past 12 months, how often have you had to provide assurance to clients that your own Business Continuity arrangements are sufficient? (N=270)

Business continuity has increasingly figured in conversations among organizations and their suppliers as well, with more than four out of 10 organizations (43%) claiming that business continuity is integrated into their procurement process. The percentage of organizations that do not mention business continuity in supplier discussions has also dropped from 31% to 18% (Figure 24). These are encouraging figures which underscore the importance of closer collaboration between business continuity and supply chain management functions.



43%
YES, it is an integral part of our procurement process from the start

24%
YES, but only where the contract risk is deemed high

15%
YES, but after the purchase decisions have essentially been taken

18%
NO

Figure 24: Question 27. Does business continuity feature as part of your supplier contractual discussions? (N= 268)

Respondents share their experiences in this area.

"Asking for business continuity arrangements among our suppliers really depends on if it relates to a product for resale or something we consume as a business."

"Recommendations have been made to inquire about business continuity planning status and we require it during procurement."

"For IT service continuity, I review requirements and capabilities annually or at contract renewal."

"Business continuity requirements are written into tender documents and reviewed as part of our vendor selection process. It also forms part of regular vendor discussions."

An expert weighs in

Nick Wildgoose FCA FCIPS

How do you compare in terms of your supply chain risk management maturity?

As this report has illustrated, the risk of disruption in your supply chain remains at a high level. Sometimes as disruptions occur just being one step ahead of your competitor can be enough. In this case study, I want to highlight how a number of organizations are not only assessing themselves but also their critical suppliers. They are using a simple Excel-based maturity model.

The Supply Chain Risk Leadership Council (SCRLC) Supply Chain Risk Management Maturity Model was designed by leading practitioners to help managers assess their organization's capabilities with respect to managing supply chain risk.

The maturity model allows a self-assessment of supply chain risk management (SCRM) capabilities across five categories (Leadership, Planning, Implementation, Evaluation, and Improvement), assessing each on a five-stage rating scale (Reactive, Aware, Proactive, Integrated, Resilient). The model is easy to use and produces three output charts that highlight the overall capability of an organization to manage supply chain risks. It has been updated in 2017 to include the important capability of supply chain mapping, which is particularly important in respect of critical supply chains.

The link to the model may be found here: **www.scrlc.com**.

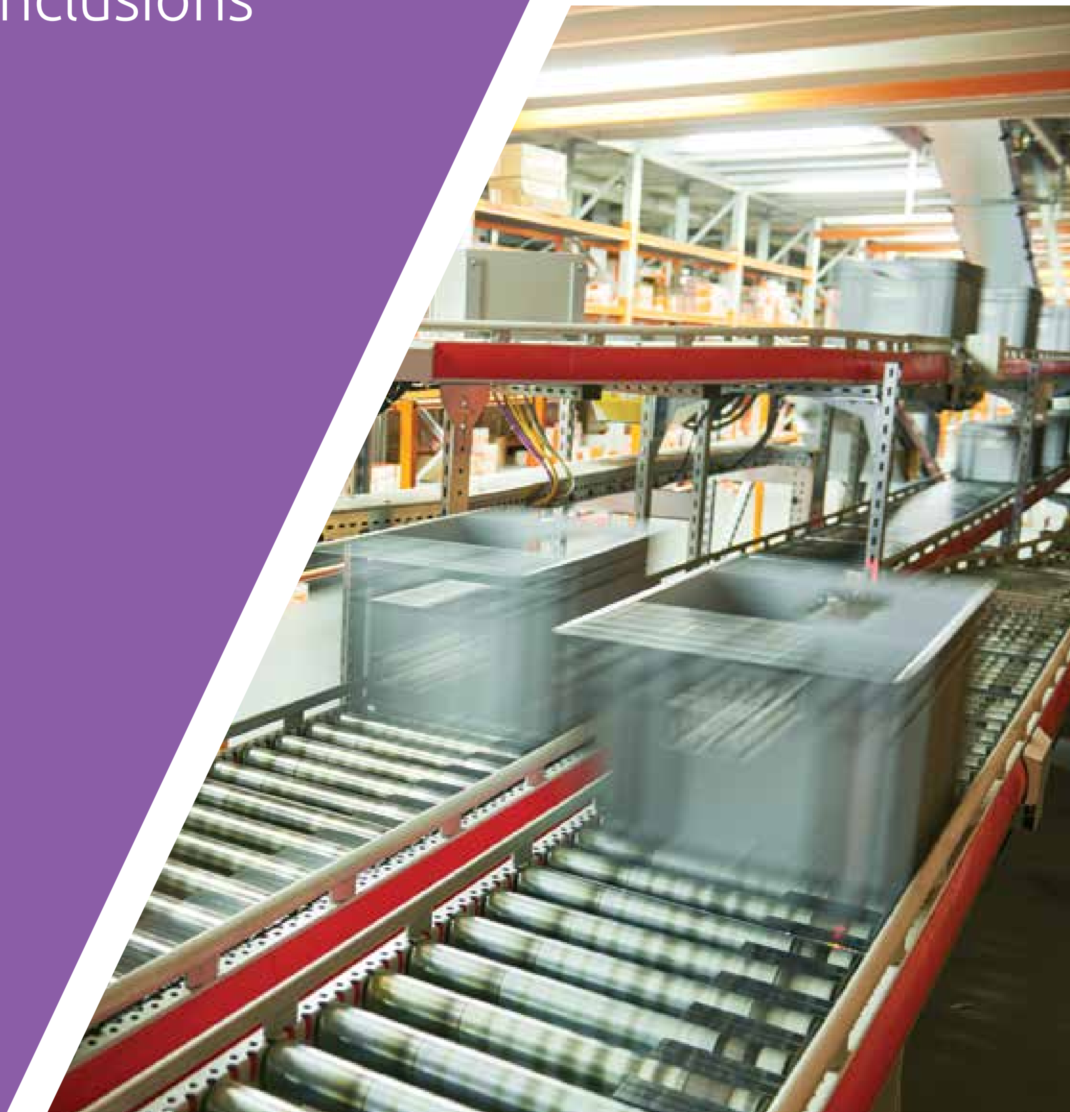
The organizations making use of this maturity model are seeing a number of benefits:

1. It provides a framework and checklist in terms of what might be the most important areas to focus on next;
2. It provides a good communication mechanism both internally and where appropriate around discussions with critical suppliers;
3. It is also a useful addition to a business case to senior management in terms of getting further investment to drive supply chain resilience;
4. It supports discussion with appropriate third parties around your supply chain resilience and for example financing or insurance; and
5. It helps everyone appreciate across the different functional areas the roles they can play in the journey to improve supply chain resilience.

About the Contributor:

Nick Wildgoose FCA FCIPS is the Global Supply Chain Product Leader at Zurich. He is a qualified accountant and supply chain professional. He served on the Board of the Chartered Institute of Procurement and Supply and as a specialist advisor to the World Economic Forum on the topic of systemic supply chain risk. He was also Chairman of the Supply Chain Risk Leadership Council, a select group of multinational companies looking to improve supply chain risk management.

4 Conclusions



Conclusions

The BCI Supply Chain Resilience Report in association with Zurich has been a comprehensive resource for business continuity, supply chain management and resilience practitioners alike for its insights on supply chain disruptions. Over the last nine years, it has also provided practical, actionable advice which enables organizations across industry sectors worldwide to improve the resilience of their supply chains. The following insights summarise some of the key points raised in the study.

1 **Technology and big data can be leveraged to overcome the skills and resources gap that hampers the effective tracking of global supply chains.**

2 **Insuring against supply chain losses is becoming a more popular option for organizations, although its uptake is variable at best.** The percentage of organizations who fully insure against the impact of supply chain disruption is at its highest in recent times and might be due to the increasing availability of insurance products in the market. Nonetheless, a majority of organizations still do not insure against supply chain disruption at all, which is an interesting area of study as to the drivers of such behaviour.

3 **The reputational aspect around supply chain disruption is still important and resonates among many organizations.** Media coverage around supply chain disruption often focuses more on organizations being supplied to and less on suppliers. For better or worse, this is a burden which requires organizations to become more aware of the issues around their supply chains and communicate effectively in times of crises in order to maintain their reputation and avert any backlash which negatively affects their brand.

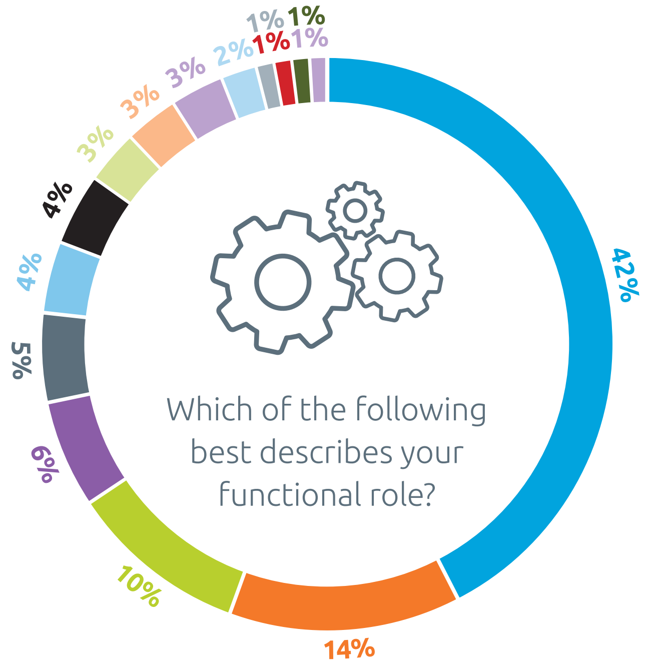
4 **Business continuity remains essential to building supply chain resilience.** This year's figures show the growing uptake of business continuity plans and arrangements related to dealing with supply chain incidents. Organizations are also increasingly looking at the business continuity plans and arrangements of their suppliers during the contract and procurement process. This proves that business continuity practitioners certainly have something to bring to the table – not least their planning and exercising skills – in terms of building supply chain resilience.

5 **Organizations are challenged to integrate relevant functions, frameworks and techniques in order to build supply chain resilience.** A lot of respondent feedback pointed out how individual functions (e.g. business continuity, supply chain and procurement, risk management, etc.) are great on their own but struggle with collaboration which hampers effective supply chain management. With organizational resilience guidance stressing the importance of joined up action, it also applies to supply chain management with relevant disciplines taking the lead in building that collaboration to improve performance.

5 Annex

Demographic information

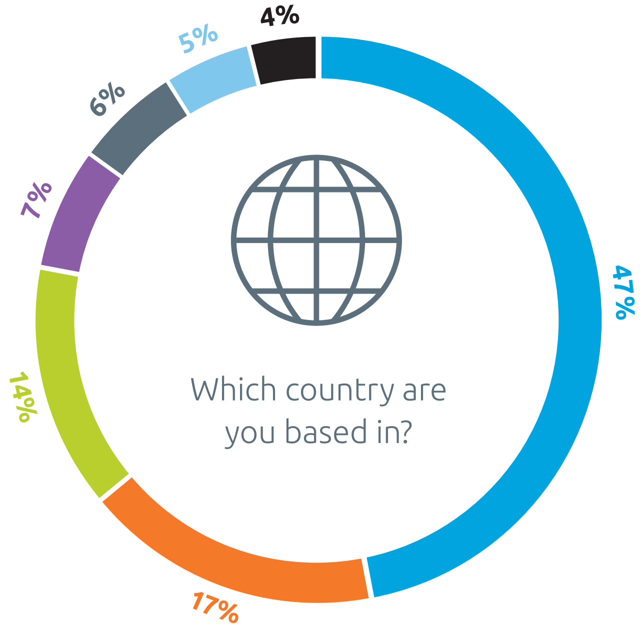
a. Functional Role of Respondents



42%	Business Continuity "in-house"
14%	Business Continuity consultant
10%	Risk Management "in-house"
6%	Supply Chain/Procurement/ Purchasing/Buyer "in-house"
5%	Security (physical/ virtual)
4%	Risk Management consultant
4%	Quality/Business Improvement
3%	Emergency Planning
3%	IT Disaster Recovery/ IT Service Continuity
3%	Supply chain/logistics "in-house"
2%	Supply chain/logistics consultant
1%	Internal Audit
1%	Line of Business/ Service Directorate
1%	Supply Chain/ Procurement consultant
1%	Health & Safety management

Question 1: Which of the following best describes your functional role? (N=408)

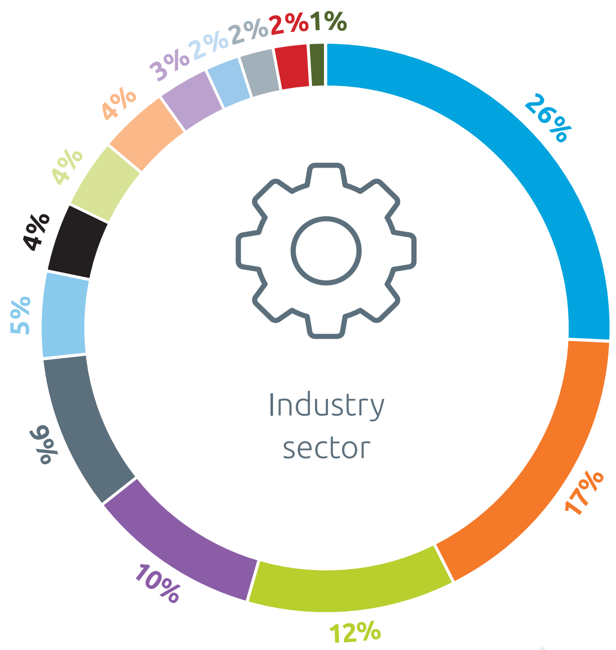
b. Geographical Base



47%	Europe
17%	North America
14%	Asia
7%	CALA
6%	Australasia
5%	Sub Saharan Africa
4%	MENA

Question 2: Which country are you based in? Please select from the dropdown menu. (N=408)

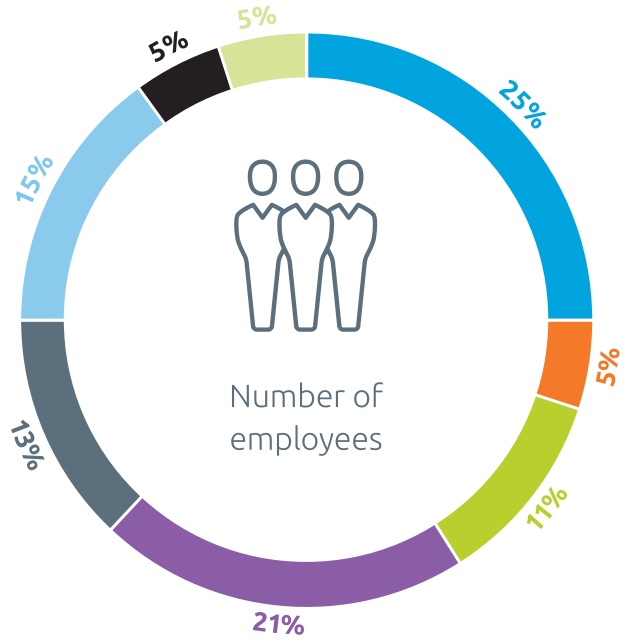
c. Industry Sector



Question 3: Please indicate the primary activity of your organization using the SIC 2007 categories given below. (N=408)

26%	Financial & Insurance Services
17%	Professional Services
12%	IT & Communications
10%	Public Administration & Defense
9%	Manufacturing
5%	Retail & Wholesale
4%	Transport & Storage
4%	Health & Social Care
4%	Energy & Utility Services
3%	Education
2%	Media & Entertainment
2%	Life Sciences/ Pharmaceuticals
2%	Engineering & Construction
1%	Support Services
0%	Mining & Quarrying
0%	Agriculture, Forestry & Fishing

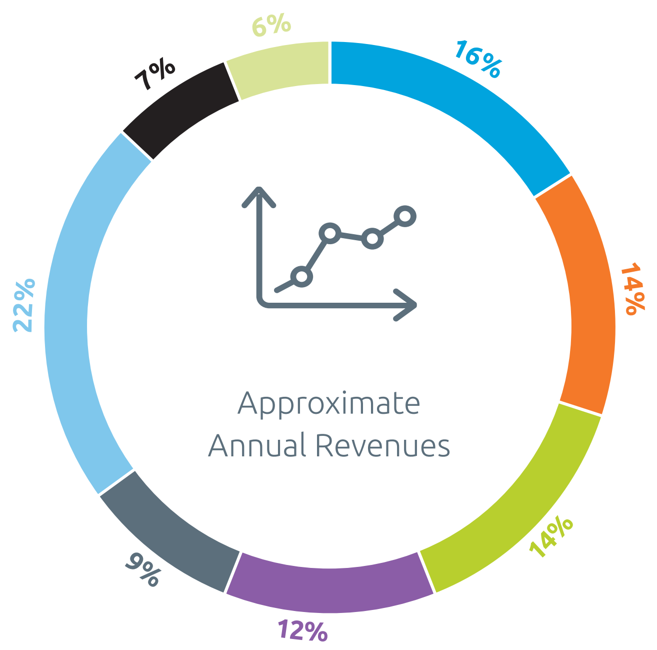
d. Number of employees



25%	0-250
5%	251-500
11%	501-1,000
21%	1,001-5,000
13%	5,001-10,000
15%	10,001-50,000
5%	50,001-100,000
5%	Greater than 100,000

Question 4: Approximately how many employees work at your organization? (N=408)

e. Approximate Annual Revenues



16% Less than €1 million	14% €1-10 million
14% €11-100 million	12% €101-500 million
9% €501 million-€1 billion	22% €1-10 billion
7% €11-50 billion	6% Greater than €50 billion

Question 5: If you are a working in a private sector organization, please let us know the approximate annual revenues of your business. (N=408)

Causes of disruption

a. By Region/Country

Rank	Europe	North America	Australasia	CALA
1	Unplanned IT or telecommunications outage (48%)	Unplanned IT or telecommunications outage (47%)	Adverse weather (46%)	Unplanned IT or telecommunications outage (57%)
2	Loss of talent/skills (35%)	Cyber attack and data breach (41%)	Unplanned IT or telecommunications outage (42%)	Outsourcer failure (52%)
3	Cyber attack and data breach (34%)	Adverse weather (39%)	Earthquake/tsunami (33%)	Cyber attack and data breach (52%)
4	Outsourcer failure (33%)	Outsourcer failure (31%)	Cyber attack and data breach (25%)	Loss of talent/skills (48%)
5	Adverse weather (31%)	Loss of talent/skills (31%)	New laws or regulations (21%)	Business ethics incident (48%)

Rank	MENA	Sub-Saharan Africa	Asia	UK
1	Unplanned IT or telecommunications outage (50%)	Unplanned IT or telecommunications outage (59%)	Unplanned IT or telecommunications outage (49%)	Unplanned IT or telecommunications outage (45%)
2	Loss of talent/skills (43%)	Loss of talent/skills (41%)	Loss of talent/skills (47%)	Outsourcer failure (27%)
3	Transport network disruption (43%)	Currency exchange rate volatility (41%)	Outsourcer failure (47%)	Insolvency in the supply chain (23%)
4	New laws or regulations (43%)	Outsourcer failure (35%)	Transport network disruption (40%)	Loss of talent/skills (21%)
5	Product quality incident (36%)	Energy scarcity (35%)	Adverse weather (38%)	Cyber attack and data breach (20%)

Rank	US	India	Canada	Australia
1	Unplanned IT or telecommunications outage (45%)	Unplanned IT or telecommunications outage (69%)	Unplanned IT or telecommunications outage (54%)	Unplanned IT or telecommunications outage (50%)
2	Cyber attack and data breach (42%)	Loss of talent/skills (50%)	Adverse weather (46%)	Adverse weather (36%)
3	Adverse weather (37%)	Transport network disruption (50%)	Cyber attack and data breach (38%)	Cyber attack and data breach (29%)
4	Outsourcer failure (34%)	New laws or regulations (44%)	Loss of talent/skills (31%)	New laws or regulations (21%)
5	Loss of talent/skills (32%)	Outsourcer failure (44%)	Transport network disruption (31%)	Outsourcer failure, Civil unrest/conflict, Loss of talent/skills, Energy scarcity (14%)

b. By industry

Rank	Financial & Insurance Service	Professional Services	IT & Communications
1	Unplanned IT or telecommunications outage (69%)	Loss of talent/skills (39%)	Unplanned IT or telecommunications outage (62%)
2	Cyber attack and data breach (43%)	Unplanned IT or telecommunications outage (37%)	Cyber attack and data breach (49%)
3	Loss of talent/skills (34%)	Cyber attack and data breach (34%)	Loss of talent/skills (43%)
4	Outsourcer failure (33%)	New laws or regulations (32%)	Outsourcer failure (41%)
5	Adverse weather (33%)	Energy scarcity (32%)	New laws or regulations (38%)

Rank	Public Administration	Manufacturing	Retail & Wholesale
1	Unplanned IT or telecommunications outage (56%)	Outsourcer failure (64%)	Adverse weather (38%)
2	Adverse weather (38%)	Product quality incident (43%)	Product quality incident (31%)
3	Outsourcer failure (35%)	Transport network disruption (39%)	Fire (31%)
4	Loss of talent/skills (35%)	Loss of talent/skills (39%)	Currency exchange rate volatility (31%)
5	Insolvency in the supply chain (29%)	Insolvency in the supply chain (36%)	New laws or regulations, Unplanned IT or telecommunications outage (25%)

Rank	Financial & Insurance Service	Professional Services	IT & Communications
1	Unplanned IT or telecommunications outage (69%)	Loss of talent/skills (39%)	Unplanned IT or telecommunications outage (62%)
2	Cyber attack and data breach (43%)	Unplanned IT or telecommunications outage (37%)	Cyber attack and data breach (49%)
3	Loss of talent/skills (34%)	Cyber attack and data breach (34%)	Loss of talent/skills (43%)
4	Outsourcer failure (33%)	New laws or regulations (32%)	Outsourcer failure (41%)
5	Adverse weather (33%)	Energy scarcity (32%)	New laws or regulations (38%)

c. By Size of Business

Rank	SMEs	Large Enterprises
1	Unplanned IT or telecommunications outage (41%)	Unplanned IT or telecommunications outage (51%)
2	Outsourcer failure (38%)	Cyber attack and data breach (36%)
3	Loss of talent/skills (37%)	Adverse weather (34%)
4	Cyber attack and data breach (31%)	Loss of talent/skills (33%)
5	New laws or regulations (29%)	Outsourcer failure (31%)

About the Authors

Patrick Alcantara DBCI
(BCI Research & Insight Lead)

Patrick heads the research department of the BCI. He is a senior research practitioner with extensive publication, project management and public speaking experience. He has delivered research projects for organizations such as the Zurich Insurance Group, PwC, Regus and the UK Department of Business Innovation & Skills. He is also part of the Editorial Board of the international, peer-reviewed Journal of Business Continuity & Emergency Planning. He obtained a Diploma in Business Continuity Management and a Bachelor degree in Psychology. He was also awarded a Distinction for a Masters by the Institute of Education (now University College London) and Deusto University.

He can be contacted at patrick.alcantara@thebci.org.

Gianluca Riglietti CBCI
(BCI Research & Insight Associate)

Gianluca has a Masters in Geopolitics, Territory and Security from King's College London. He has experience writing academic and industry publications, speaking at international conferences, and delivering projects for companies such as BSI, Everbridge, and Transputec. His previous professional experience includes working for the Italian Presidency of the Council of Ministers.

He can be contacted at gianluca.riglietti@thebci.org.

Lucila Aguada
(BCI Research & Insight Assistant)

Lucila is a licensed psychometrician with expertise in quantitative and qualitative research. She has a Bachelor degree and is a Masters candidate in Psychology from the University of the Philippines. She has conducted research on behalf of non-profits, pharmaceutical and healthcare clients. She is also a qualified teacher with more than seven years of experience, specialising in early childhood and special needs education.

She can be contacted at lucila.aguada@thebci.org.

Acknowledgements

The BCI is grateful for the efforts of the **Chartered Institute of Procurement and Supply (CIPS)** for promoting the 2017 Supply Chain Resilience Survey.

We would also like to thank **Zurich** for supporting this research for the ninth year running.

We also acknowledge the support given by the following individuals during the survey fieldwork. **Nick Wildgoose, Shilpa Freemantle (Zurich) and Trudy Salandiak (CIPS)** assisted in disseminating the survey. **Nick Wildgoose and Matthew Hillyer (Zurich)** provided case studies. **Kuniyuki Tashiro MBCI** (Business Continuity Institute) translated the survey questionnaire into Japanese.

About the BCI

Founded in 1994 with the aim of promoting a more resilient world, the Business Continuity Institute (BCI) has established itself as the world's leading Institute for business continuity and resilience. The BCI has become the membership and certifying organization of choice for business continuity and resilience professionals globally with over 8,000 members in more than 100 countries, working in an estimated 3,000 organizations in the private, public, and third sectors.

The vast experience of the Institute's broad membership and partner network is built into its world class education, continuing professional development and networking activities. Every year, more than 1,500 people choose BCI training, with options ranging from short awareness raising tools to a full academic qualification, available online and in a classroom. The Institute stands for excellence in the resilience profession and its globally recognised Certified grades provide assurance of technical and professional competency. The BCI offers a wide range of resources for professionals seeking to raise their organization's level of resilience, and its extensive thought leadership and research programme helps drive the industry forward. With approximately 120 Partners worldwide, the BCI Partnership offers organizations the opportunity to work with the BCI in promoting best practice in business continuity and resilience.

The BCI welcomes everyone with an interest in building resilient organizations from newcomers, experienced professionals and organizations. Further information about the BCI is available at www.thebci.org.

About Zurich

Zurich is a thought leader in supply chain risk management. It has developed supply chain risk assessment tools and an innovative and award winning supply chain insurance product. The company has extensive experience of working with clients to help them make their supply chains more resilient.

Zurich Insurance Group (Zurich) is a leading multi-line insurance provider with a global network of subsidiaries and offices in Europe, North America, Latin America, Asia-Pacific and the Middle East as well as other markets. It offers a wide range of general insurance and life insurance products and services for individuals, small businesses, mid-sized and large companies as well as multinational corporations. Zurich employs about 60,000 people serving customers in more than 170 countries. Founded in 1872, the Group is headquartered in Zurich, Switzerland. Zurich Insurance Company Ltd (ZURN) is listed on the SIX Swiss Exchange and has a level I American Depositary Receipt program (ZFSVY) which is traded over-the-counter on OTCQX.

For further information about Zurich, go to: www.zurich.com.

Contact the BCI

Marianna Pallini

Communications Executive

+44 118 947 8215 | **research@thebci.org**

10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.

Contact Zurich

Nick Wildgoose

Global Supply Chain Product Leader

+44 (0) 20 7648 3066 | **nick.wildgoose@uk.zurich.com**

Zurich Insurance PLC, 70 Mark Lane, London EC3R 7NQ, United Kingdom

Business Continuity Institute

Business Continuity Institute

10-11 Southview Park, Marsack Street,
Caversham, Berkshire, UK, RG4 5AF

bci@thebci.org
www.thebci.org

Correct as of November 2017

ZURICH