6th Annual DRI International Global Risk and Resilience Trends Report

Report Methodology

The DRI International Global Risk and Resilience Trends Report is now in its sixth year. The 2020 report and survey have been extended from previous years to include an additional section dedicated to Covid-19. Questions were asked about how prepared organizations were for the pandemic and how much they agreed with certain statements about the post Covid-19 situation.

Supported by the DRI Future Vision Committee (FVC), the report gives an independent analysis of both external issues (current and emerging risks) and internal concerns (resilience management as a profession). The FVC consists of international thought leaders and experts in all aspects of resilience management.

Opinion is provided via an annual survey of professionals who work in various resilience and management roles across many countries, business sectors, and government agencies. The main components of resilience are business continuity, disaster recovery, crisis management, and emergency management. These form the basis of resilience management, but to be most effective they also require strong links to risk management and security. Participants from these areas, as well as information technology (IT), facilities, human resources (HR), procurement, compliance, and audit participated in the survey.

The survey was based upon an initial set of issues defined by the FVC members. Both DRI Certified Professionals and other experienced resilience practitioners in related fields participated. The committee identified 20 key risks and asked participants for their opinions. This annual report feeds the knowledge base, which is central to the growth of an integrated resilience discipline. Feedback from business, academia, media, and government indicate that the report also provides significant insight for the wider business community. Increasingly, DRI International is emerging as a major source of knowledge and expert opinion for a range of national and global media outlets. This report provides a core part of DRI's knowledge management and external messaging.

Executive Summary

A unique year, 2020 was dominated by Covid-19. By mid-February, outbreaks in parts of Europe signalled that this new virus could become a global crisis. Declared an official global pandemic by the World Health Organization (WHO) on March 11, Covid-19 was still sweeping the globe during a second wave as of this publication date in December.

Risk and Preparedness

Last year's report saw pandemics being viewed as a medium risk in terms of probability and impact, ranking just 13th on the resilience index. In the 2020 report, pandemics have risen to the top spot on the same index. However, the impact of Covid-19 is far from equally-shared across sectors. For some industries, Covid-19 has not presented the operational challenges many expected. Technologies supporting work from home (WFH) and virtual conferencing have graduated from little-used tools to the primary way of operating for industries that are largely information-based. Other sectors, such as travel, hospitality, and entertainment, struggle to survive as government Covid-19 suppression measures combined with dwindling customer demand make business as usual impossible.

Due to the criticality of this issue, this year's report includes an additional section dedicated to Covid-19. Questions were asked about how prepared organizations were for the pandemic, how they performed, and how much they agreed with certain statements about the post Covid-19 situation. The results show that while few organizations had prepared comprehensively for such an extensive and extended crisis, the vast majority believe they handled it well.

Economic Impact

While there is significant regard for medical issues, the greatest pandemic-related concern for resilience professionals is its economic impact. Traditionally, technological risk issues have been the main driver of resilience planning, but both social and political risk factors are now becoming equally crucial. Of those organizations that survive this extended emergency – and it looks like the pandemic will run well into 2021 – many will make major changes to their business models.

Current emergency measures will likely become permanent, and extensive cost-cutting seems inevitable. Regulated firms have more confidence in their ability to survive a crisis. Perhaps the reasons for this is two-fold: they are often better prepared than non-regulated firms, and they may provide key services to government. In general, the majority of survey respondents were optimistic that their organization would survive and recover well.

Supply Chain Disruption

An issue drawing increased attention this year is the serious consequences of a major supply chain disruption. Clearly, the global pandemic is already having an impact on international supply chains. Entry restrictions are tightening in many countries, and crews, at times, are unable to leave or enter their vessels. There is a danger of international shipping routes facing even more restrictions in 2021. In addition to delays to manufacturing and retail operations, supply chain risks include deliberate product contamination as well as malware attacks to customer infrastructure. In the short-term, there is also the potential for shipping disruptions in Europe if there is failure to agree a suitable trade deal between the UK and the EU.

Despite all of this, relatively few respondents in the survey believe that Covid-19 will bring lasting, fundamental changes to supply change policy beyond that which has already happened. Globalization is unlikely to be reduced by any significant degree, despite the vulnerabilities exposed by Covid-19. For a full list of questions, answers, and analysis on the pandemic, see The Covid-19 Survey Results on pages 6-9.

Cyber Crime

Concentration on Covid-19 does not mean that other risks have diminished. In fact, some have increased. The global attention paid to fighting Covid-19 has provided opportunities for cyber criminals and fraudsters to operate more freely. However, when we look at this year's Resilience Index, it is clear that priorities for many resilience practitioners have changed. They are now more concerned about availability issues, such as long-term IT outages, major operational incidents, and state-sponsored attacks on critical national infrastructure. There is less emphasis on integrity and confidentiality issues this year, with data security dropping to number 6 on the index.

Natural Disasters

Natural disasters and adverse weather events have always been near the top of the resilience index, but this category has traditionally covered a wide range of different problems. This year we gave two specific types of weather event (wildfires and seismic) their own categories. Severe weather events in this survey now cover hurricanes, typhoons, tornadoes, cyclones and similar wind/storm related issues. Wildfires also scored well, which was not surprising given the extent to which such events occurred in 2020. Although unrelated, the year saw an unusually broad spread of wildfires from Australia in January, Indonesia in mid-year and California, Oregon and Washington State in late summer.

Activism

In 2019, the report was concerned about the potential growth of activism. We concluded that political, environmental and anti-capitalist activism, encouraged by social media, were presenting more and more of a threat to operational continuity. This year, that proved true, with protests impacting business activities internationally.

Emerging Issues

Two emerging issues, with which a typical resilience function might not yet be involved, were added to the report this year. They are: the ability to ensure that new AI-based technologies would be managed in an ethical manner; and problems that may arise from increased concentration of risk in mega-cities. In fact, this trend might be mitigated by the changes in work methods, thus reducing the need for cities to grow dramatically. As the concept of a Chief Resilience Officer becomes more mainstream in business, strategic issues of this nature are likely to become part of the expanded resilience portfolio.

Figure 1: The Summary Resilience Index shows top risks for 2020 based on both likelihood and impact

1 Pandemics

2 IT Long-term Outages

3 Operational Incidents

4 Economic Failure

5 CNI State Sponsored Attack**

6 Theft of Proprietary Data

7 Severe Weather Events(*)

8 Serious Supply Chain Disruption

9 Misuse of Data

10 Wildfires

*Excluding Wildfires and Seismic Events which now have their own categories.
**(CNI) Critical National Infrastructure

Year Over Year

Comparisons of the 2020 rankings with those of 2019 are interesting. They show how quickly our perceptions have changed. Five issues have risen by four or more places in the resilience index: pandemics, supply chain disruptions, protests or civil unrest, state-sponsored cyber attacks, and the business impact of an economic downturn. We are in new territory and our priorities have been completely re-written.

Some positive take-aways were revealed this year. Confidence in senior manager's ability to manage a crisis has increased rapidly. Resilience as a profession is being more widely understood and appreciated by senior management. And the demand for resilience certification is increasing globally, with demand for high-quality resilience management programs evident in all regions and business sectors.

The 2020 Top 10

Based on a combination of likelihood and impact, the 10 resilience issues this year are radically different from 2019's list (see page 5). These issues are not necessarily risks in the conventional sense; they are the chief concerns expressed by resilience professionals and indicate where they feel they should be concentrating their efforts and resources. Every organization has been challenged, and every leadership team put under extensive stress to lead their companies through the Covid-19 crisis. As a result, views this year are likely to be much more accurate and valuable, based more on observation and evidence, rather than on opinion and conjecture.

Figure 2: Key resilience issues

Rank	Icon	Short reference	Issue description
1		Severe Weather Events	Hurricanes, tornadoes, typhoons, cyclones etc.
2		Seismic Incidents	Volcanoes, earthquakes, and tsunamis
3		Wildfires	All causes and consequences including related flooding
4		Climate Change	Short and medium-term disruptive impacts
5		Operational Incidents	Major operational incidents such as fire, explosion, or collision
6		Serious Supply Chain	Supply shortages, vendor failures, supply route interruptions
7		Management Failure	Lack of effective leadership in a major crisis situation
8		Regulatory Penalties	Fines and actions up to loss of license to operate
9		Economic Failure	Recession, depression, bankruptcy, insolvency
10		Ethics and Trust	Concerns about misuse of AI, biotech, genetics, etc.
11		Political Leadership Failure	Geopolitical failures of leadership and governance
12		Concentration of Risk	Concentration of risk in metropolitan hubs
13		Pandemic	Pandemics and epidemics – all types, causes, origins
14		Social Media Attack	Targeted social media attack on specific organization
15		Terrorism	All physical attacks up to and including CBRN attacks
16		Civil Unrest, Protests	Severe civil unrest and protest activism
17		IT Long-term Outages	Denial of access to or use of essential IT services
18		Theft of Proprietary Data	Cyber attacks to steal data or introduce malware
19		Misuse of Data	Commercial, financial and reputational damage
20		CNI State Sponsored Attack	Attacks by state actors on critical national infrastructure

The Covid-19 Survey Results

Questions were asked about how prepared organizations were for the pandemic, how effectively they responded, and how involved resilience professionals were in different phases of the response.

Question 1

*At what stage of the Covid-19 pandemic were you and your department involved?**

	%
Reviewing possible impacts as the virus emerged in China	55.85%
Producing situational data for leadership as the virus spread	61.13%
Developing a corporate strategic response	72.45%
Implementing the operational response	77.36%
Providing feedback to leadership on the effectiveness of the response	72.08%
Not involved	8.30%

*Multiple answers were permitted.

While it is a little concerning that 8.3% reported no involvement at all, the resilience community seems to have been involved extensively in all phases of the pandemic response. It is encouraging that over 72% of respondents were part of the strategic response planning and over 77% were responsible for implementing the operational response. It is clear that in many organizations, they were involved at a very early stage, a sign that senior management had trust in and expectations from their resilience specialists. One respondent felt that this “showed BC must be at the heart of any business, Covid-19 clearly demonstrates that.”

There were no significant differences between regions and sectors, except for Latin America where initial involvement was lower than elsewhere; involvement at both strategic planning and operational implementation was in-line with all other regions.

Question 2

When the virus first emerged did you have a pandemic plan in place?

	%
Yes, but it was basic and untested	27.17%
Yes, it was detailed, but based on assumptions from previous epidemics	29.81%
Yes, it was comprehensive, regularly tested, but didn't account for such a widespread global impact	10.94%
Yes, it was comprehensive, regularly tested, and included the potential global impact in our planning	6.42%
No, we never considered this risk as significant	12.08%
No, but we started to develop one immediately	13.58%

The general indication from these results is that companies were not very well prepared for Covid-19, with only 6.42% indicating that they had an effective, comprehensive plan in place. In fact, 25.66% had no pandemic plan at the start of the crisis. The most common answer was that the pandemic plan was based on assumptions from previous pandemics and epidemics. The second most common response was that the plan that existed was basic and untested. One respondent made the point that “probably no-one was fully prepared – the scale was bigger than anyone believed could happen.” Nevertheless, it was a disappointing result given the inevitability of a global pandemic happening at some point. It has been well-signalled by both government agencies and the media for many years. Close calls with other coronaviruses like SARS and MERS should have triggered a more sustained approach to planning against this high impact risk.

Again, there was little difference between regions although the Far East has slightly the best record in terms of having a comprehensive plan and Latin America marginally the worst. North America, Europe and Middle East gave similar responses to this question.

Question 3

How well do you think your organization has handled the Covid-19 crisis?

	%
Very well, we were ready for it and acted quickly and effectively	46.79%
Reasonably well, we did all we could in difficult circumstances	35.47%
Adequately, we could have been better prepared and acted earlier	13.21%
Poorly, we underestimated the problem and failed to get control of the situation	4.53%

It appears from these results that companies tended to do better than expected based on their level of planning. Only 4.5% felt they performed poorly against over 25.6% who had no plan at the start of the pandemic. One participant noted “many things happened simultaneously and we had to constantly reassess the combined impact.”

Conversely, 46.7% felt they had performed very well when only 6.4% reported they had a comprehensive plan. Of course, these views are subjective and later review might highlight weaknesses. A positive interpretation of this data is that many companies have a high degree of embedded resilience in their organization. This allows them to respond quickly and effectively without following detailed instructions. It illustrates that the all hazards approach to planning advocated by DRI International has worked well in a situation so complex that a detailed plan would have been impractical. However, targeted planning for specific response and recovery options may have saved time and prevented some unsuccessful decisions being made.

In terms of performance, all regions and sectors felt they had performed well or very well. This perception was consistent, even in Latin America where other metrics had not been so positive. It is also difficult to make objective comparisons given that different regions and sectors might have different expectations.

Question 4

What will be the long-term business impact of Covid-19?

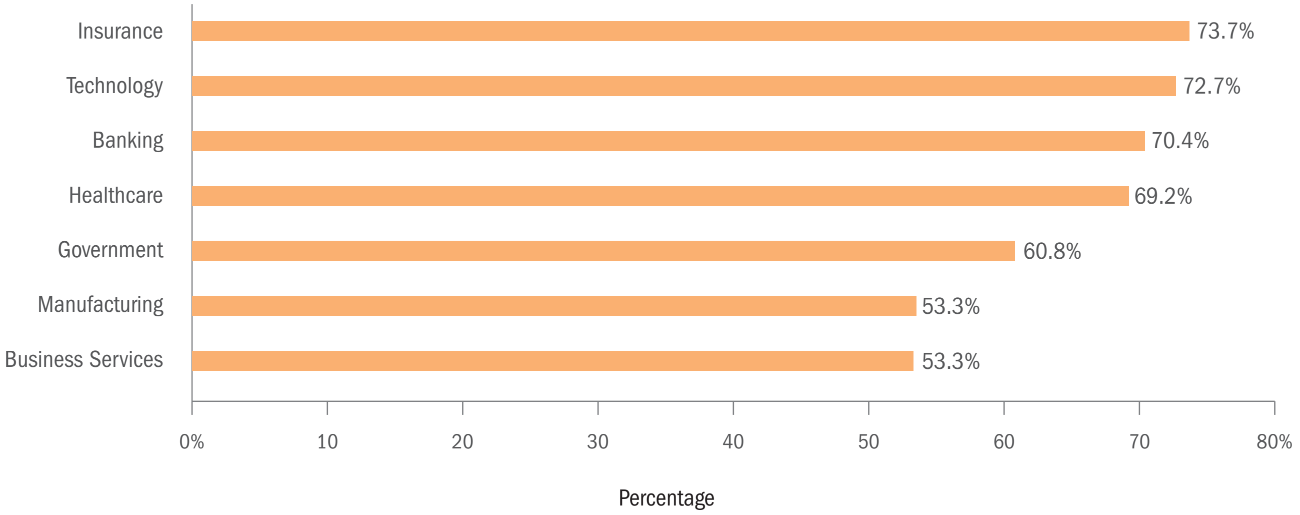
Participants were asked to respond to statements about the predicted long-term changes that might happen. These statements were all popular opinions being expressed in the business media. The FVC wanted to understand the extent to which resilience professionals agreed.

The request was “Please indicate how much you agree/disagree with each of the statements as it affects your organization. The statements are listed below in the order asked. Two ways of measuring agreement were used but they gave exactly the same ranking order. The methods were:

- a weighted average based upon a scale of and 1 (strongly disagree) to 5 (strongly agree)
- the percentage scoring Agree or Strongly Agree

There is wide-scale agreement that work from home will become a regular feature of future employment. The expectation that more optional work will be permitted by management is accepted by most participants. This does, however, vary from sector to sector. There are 21 sectors represented in the survey and we have looked at the top 7 sectors which contribute 70% of the results. In response to the expectation of more home-working being permitted the following list shows the strongly agree results for these sectors (see Figure 3, page 8).

Figure 3: In response to the expectation of more home-working being permitted the following list shows the "strongly agree" results for the top seven sectors.



Overall, some 25% strongly agreed that compulsory working from home will also be part of the new normal. One participant felt that "many project managers and engineers have worked from home for 20 years, so it was not a novel situation." Another felt "it will badly hit commercial work area recovery (WAR) services as home working is now normal."

Over 60% predicted a fundamental changes to the business model as demand patterns change, and over 50% believed there will be increased spending on resilience and business continuity as a result of the crisis.

Fewer than 50% were convinced that operations and headcount will be reduced, that less popular products will be withdrawn, that there will be less dependence of global supply chains, and that companies might struggle to survive. At a regional level, there was general agreement on most of the issues. The table below shows the order in which the various propositions are supported (1 being the most supported, 9 being least) (see Figure 4, page 9).

The seven sectors that made up over 70% of responses had the same top three expectations, and all ranked business failure as the least expected. At this time, Covid-19 has had such a strong influence on behavior and thinking that there is much more cross-sector agreement than is found on any other resilience issue. However, the impact of Covid-19 is not equal across sectors. However, if the top 3 statements are true for many companies, this is bad news indeed for airlines, other travel operators, commercial property owners, realtors, bars and restaurants, office cleaners, and all smaller companies that service large-scale city employment hubs in a myriad of ways.

The findings is Figure 3 are interesting but somewhat concerning findings. Certainly, if they are true then city-based large companies might be able to reduce operating expenses significantly, but this will increase job losses and bankruptcies in the types of businesses listed earlier. This will reduce overall economic activity and national GDP, likely causing governments to adopt policies attempting to bolster growth. The hope of few job losses, little operational

Figure 4: Order in which the various propositions are supported (1 being the most supported, 9 being least)

Statement	North America	Latin America	Europe	Middle East	Far East
More optional home-working	1	1	1	1	2
Reduced business travel	2	2	2	2	1
More compulsory home-working	3	3	3	3	3
Business model and demand changes	5	5	4	4	4
Less globalised supply chains	7	8	8	7	5
Increased resilience spending	4	6	6	5	6
Reduced product/services	8	4	7	8	7
Operations streamlining, job reductions	6	7	5	6	8
Uncertainty for business to survive	9	9	9	9	9

Figure 5: The long-term business impact of Covid-19

	Strongly agree	Agree	Unsure	Disagree	Strongly disagree	Total agree and SA	Weighted average
More optional work from home will be permitted	62.26	30.19	3.40	2.64	1.51	92.45	4.49
Business travel will be significantly reduced	33.96	46.04	14.72	4.91	0.38	80.00	4.08
More compulsory work from home will become the new normal	30.19	40.38	21.89	4.91	2.64	70.57	3.91
There will be a significant business model change to meet changing demand requirements	15.47	44.91	22.26	13.58	3.77	60.38	3.55
There will be increased spending on resilience/business continuity planning	13.21	44.53	27.17	12.45	2.64	57.74	3.53
Operations will be streamlined and headcount will be reduced	15.09	29.81	23.77	24.15	7.17	44.91	3.22
The less popular or less profitable products and/or services will be withdrawn	6.04	26.79	37.74	19.25	10.19	32.83	2.99
There will be less dependency on global supply chains	5.66	23.02	37.36	27.79	7.17	28.68	2.93
There is uncertainty about our ability to survive	3.77	13.58	12.08	31.32	39.25	17.36	2.11

streamlining, and company survival while spending more on resilience is optimistic. It must be based on the opinion that international economies can recover from the Covid-19 interruption quickly and without permanent structural damage to business or social stability. Many business and financial experts think this is doubtful. However, the speed and strength of economic recovery in China and South Korea once Covid-19 was under control gives some optimism that a similar recovery can occur elsewhere.

The 2020 survey

Geo-political Risks

As context for the detailed survey, an overview of perceived priorities across the main resilience risk categories was obtained.

The categories made available for ranking were shown in the table below, together with the average of all the rankings received. Since overriding concerns about Covid-19 would have distorted the figures, pandemics were not assigned to any specific category. The maximum score is 5, the minimum score is 1. They are listed in order of importance.

Figure 5: Full survey ranking of global risk categories by priority. Maximum score is 5, minimum score is 1, listed in order of importance.

Global Risk Category		Priority*
T	**Technological risk** — cyber attacks, IT failures, and criminal or unethical misuse of emerging technologies	3.09
P	**Political and economic risk** — financial uncertainty at global, national, local and company levels and national stability	3.07
S	**Social risk** — political activism, wide-scale protest movements, labor disputes, and civil unrest leading to serious damage	3.05
En	**Environmental risk** — negative impact of not adopting green policies with commercial, legal, and reputational damage	2.98
Op	**Operational Risk** — operational failure, internal processes, people, and/or systems disruptions	2.85

*Out of 5. Higher scores indicate higher importance.

Technological risk maintained the top score but was very closely challenged by both political and social risk. Despite the high profile of environmental risk, it dropped from 3rd to 4th place in this survey. It is clear, however, that all risk categories are considered very important by resilience professionals and are often interlinked. More information relating to how these risk categories are ranked within regions and sectors can be found further on in this report.

Probability, impact and resilience

For comparison purposes, a scale of 1 to 5 was utilized, with 1 being the lowest and 5 the highest, in terms of the importance assigned to each issue. For both PROBABILITY AND IMPACT, a simple statistical average was calculated (MEAN VALUE). To develop a “Resilience Risk Index” the probability and impact scores were multiplied. The two rankings are shown in figures 6 and 7 (page 11).

There was less correlation between the order for probability and impact than previous years. This suggests that the experience this year with the Covid-19 crisis has resulted in an upgrade of some of the prior assumptions about the maximum level of potential impact for other risks as well.

As expected, much attention was paid to pandemics. However, an extended IT outage was thought to have a larger overall business impact than pandemics by the majority of respondents. Although a state-sponsored attack on national infrastructure was considered no more probable than in previous years, the impact this would have is now perceived as much greater than before.

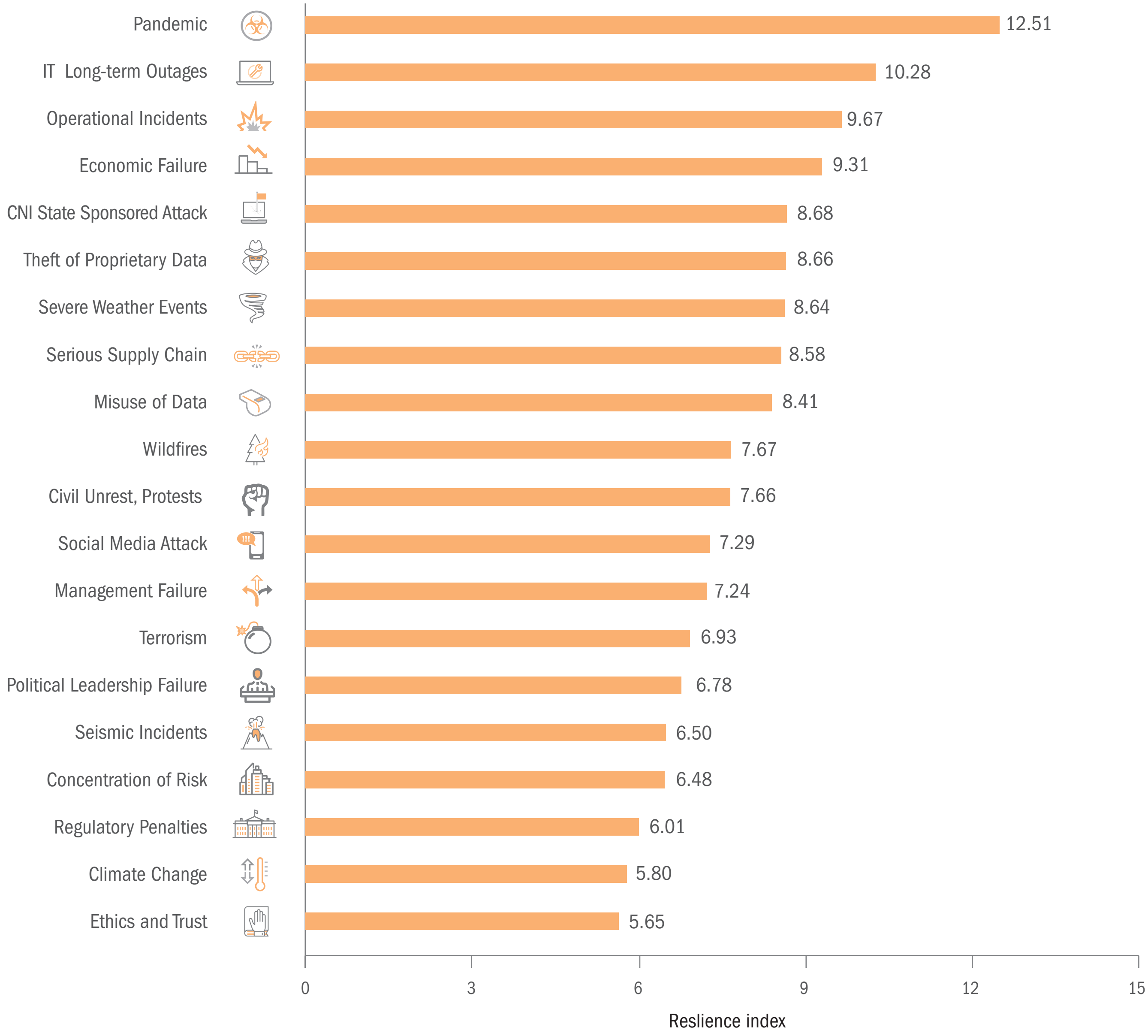
Figure 6: The PROBABILITY of the defined issue causing significant problems during 2020

Rank	Icon	Issue reference	Mean value
1		Pandemic	3.70
2		Operational Incidents	3.05
3		IT Long-term Outages	2.97
4		Severe Weather Events	2.95
5		Economic Failure	2.90
6		Serious Supply Chain	2.86
7		Wildfires	2.83
8		Theft of Proprietary Data	2.75
9		Social Media Attack	2.71
10		Civil Unrest, Protests	2.68
11		CNI State Sponsored Attack	2.67
12		Misuse of Data	2.62
13		Concentration of Risk	2.56
14		Political Leadership Failure	2.55
15		Climate Change	2.47
16		Management Failure	2.43
17		Terrorism	2.34
18		Seismic Incidents	2.29
19		Ethics and Trust	2.28
20		Regulatory Penalties	2.08

Figure 7: The IMPACT on the organization if the defined issue occurred during 2020

Rank	Icon	Issue reference	Mean value
1		IT Long-term Outages	3.46
2		Pandemic	3.38
3		CNI State Sponsored Attack	3.25
4		Economic Failure	3.21
5		Misuse of Data	3.20
6		Operational Incidents	3.17
7		Theft of Proprietary Data	3.15
8		Serious Supply Chain	3.00
9		Management Failure	2.98
10		Terrorism	2.96
11		Severe Weather Events	2.93
12		Regulatory Penalties	2.89
13		Civil Unrest, Protests	2.86
14		Seismic Incidents	2.84
15		Wildfires	2.71
16		Social Media Attack	2.69
17		Political Leadership Failure	2.66
18		Concentration of Risk	2.53
19		Ethics and Trust	2.48
20		Climate Change	2.35

Figure 8: The Resilience Index shows the top issues from the 2020 survey.



During the previous five years, we have seen relatively few changes in this index on a year-by-year basis. In 2020, it has changed massively over 2019.

The issues that have risen more than three places from 2019 are:

Pandemic	+ 12
Supply Chain Disruption	+ 6
Civil Unrest and Protests	+ 6
Impact of Economic Problems	+ 4
CNI State Sponsored Attack	+ 4

The main issue that has fallen since 2019 is:

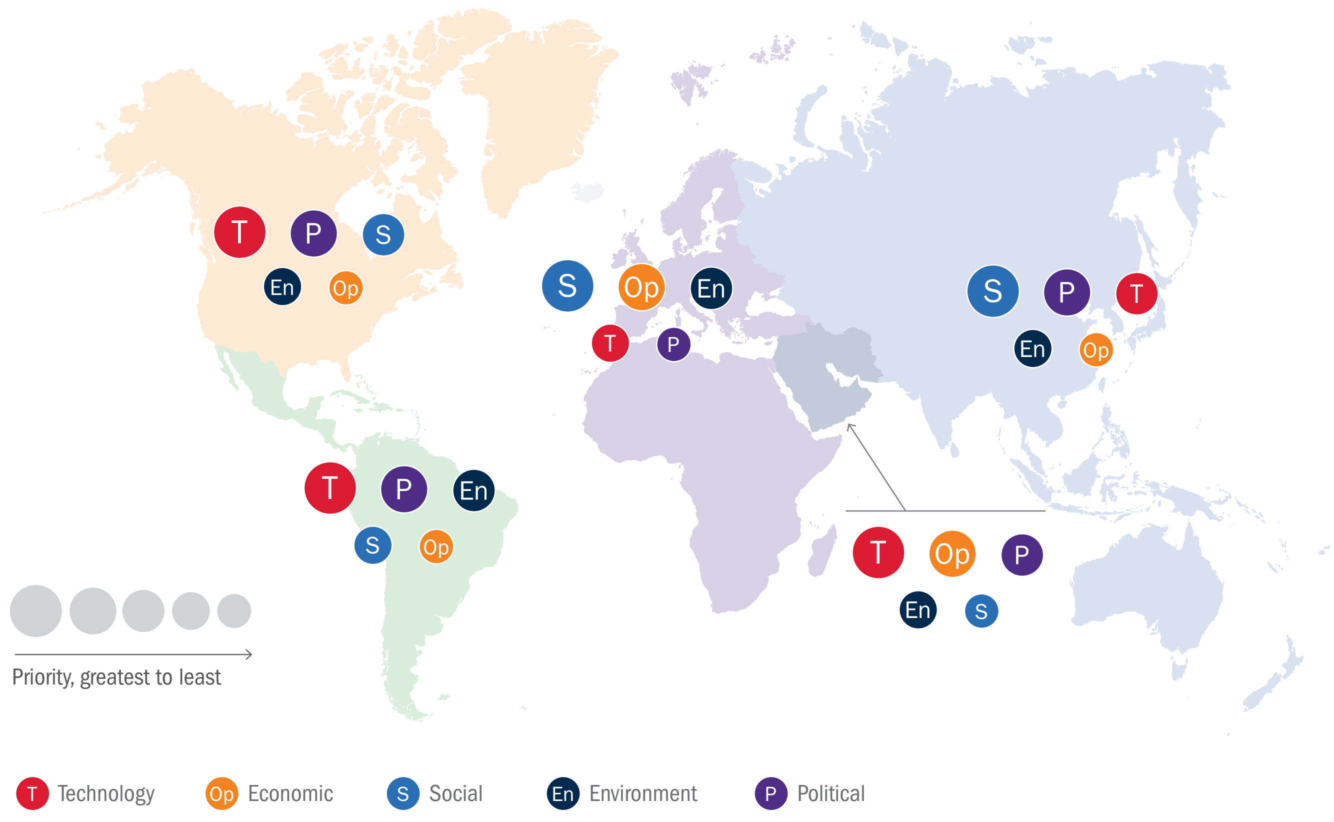
Crisis Management Failure	– 8

These results demonstrate the profound impact that Covid-19 has had on our thinking, worries, and expectations.

Regional Analysis

The survey looked at five world regions. We received responses from Australia, New Zealand, and Africa but the numbers were inadequate to include them as separate categories. They are included in the overall figures.

Figure 9: Region — Risk Category Priorities



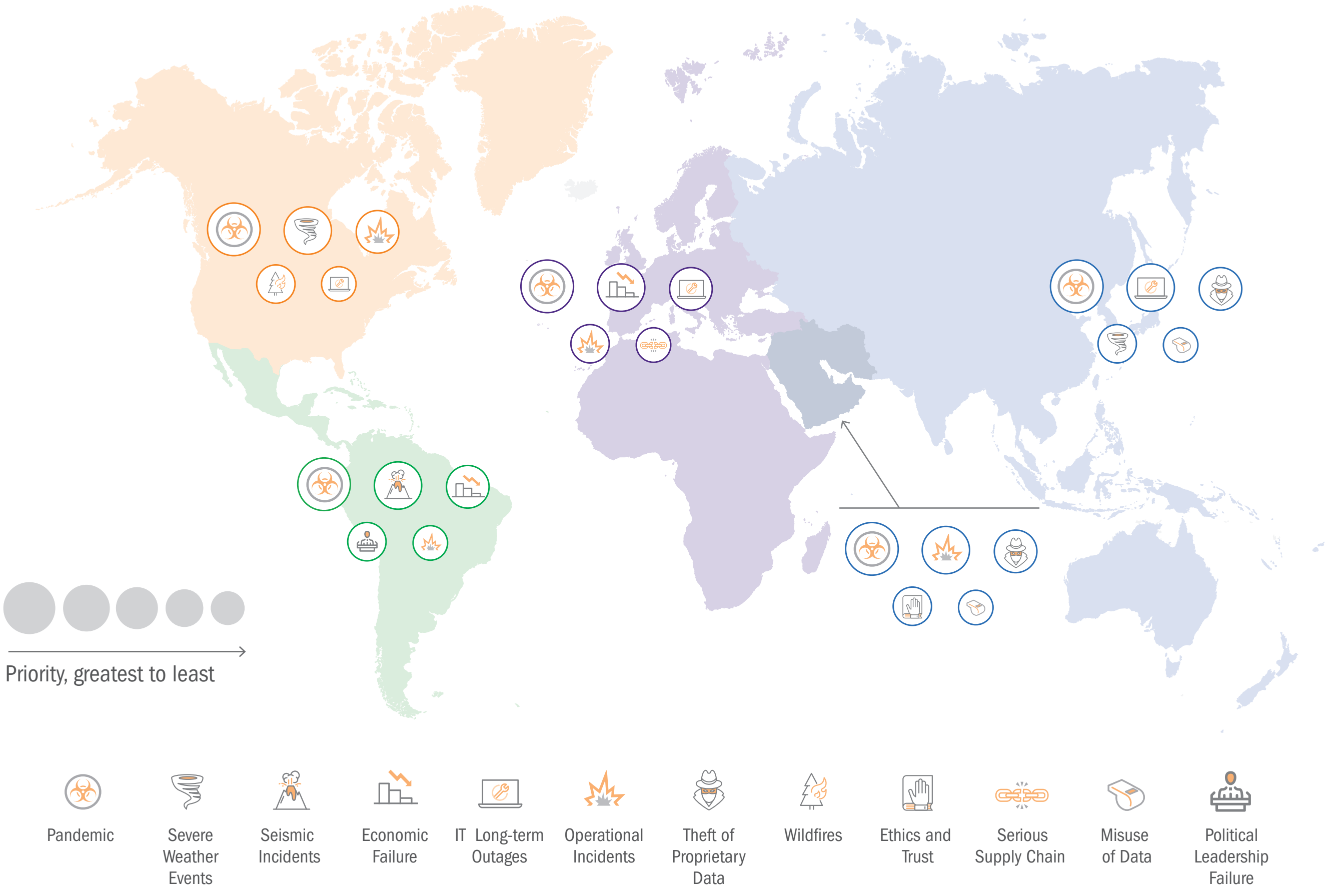
In all previous surveys, regions have shown a high level of agreement about the relative importance of different global risks. This consensus has been disrupted in 2020 and significant differences have emerged. The only explanation for this is the unique circumstances prevailing this year. Whereas technological risk has always dominated everywhere, in 2020 it was replaced in both Europe and Asia (Far East) by social risk as the major worry. In both North and Latin America technological risk stayed in top place but was very closely challenged by political risk. Operational risk also became a major issue in Europe and Asia (Middle East) but was the lowest risk concern elsewhere.

Regional resilience concerns

Figure 10, below, shows the top 5 PROBABILITY issues for each of the regions.

It is very interesting that although pandemics scored the highest probability in every region, they were not considered the highest impact issue for any region. Considered in context, 2021 will certainly bring a continuation of the pandemic crisis, justifying the top rating on the probability scale. However, many businesses suspect that they have already felt the major impacts of the pandemic impact in 2020. They have reorganized their activities to enable them to continue reasonably effectively in 2021. The impacts

Figure 10: Region – Probability Ranking



from now on will largely be outside of their control, the main one being severe and lasting economic recession.

The resilience index (combining probability and impact) for each region gives the following top 10 issues per region. Extended IT outage and economic/ financial are scoring heavily across the world.

Despite the variations in impact ratings, it is no surprise that pandemics top the resilience index for every region. The majority of regions show an extended IT outage as the next most important issue for 2021. Europe, Middle East, and Latin America have strong concerns about the economic situation resulting from Covid-19, while North America seems more confident about this issue. In Asia (Far East) economic concerns do not feature highly. Interestingly, this does seem to be in-line with the general economic expectations of the regions going into the Covid-19 crisis, which may be different post-Covid-19.

Some high scoring issues are geographically specific, such as the risk of seismic disasters in Latin America, and wind-related weather events in North America and the Far East. In the latter two regions, the risk of wildfires also appears in their top 10 – a consequence of the severe problems experienced this

Figure 11: The resilience index for each region gives the following top 10 issues per region

Resilience Index Rating	North America	Latin America	Europe	Asia Far East	Asia Middle East
1	Pandemic	Pandemic	Pandemic	Pandemic	Pandemic
2	IT Long-term Outages	Seismic Incidents	IT Long-term Outages	IT Long-term Outages	Economic Failure
3	Severe Weather Events	Economic Failure	Economic Failure	Severe Weather Events	Operational Incidents
4	Operational Incidents	IT Long-term Outages	CNI State Sponsored Attack	CNI State Sponsored Attack	Misuse of Data
5	Theft of Proprietary Data	Severe Weather Events	Operational Incidents	Theft of Proprietary Data	Theft of Proprietary Data
6	Misuse of Data	Operational Incidents	Management Failure	Operational Incidents	IT Long-term Outages
7	Economic Failure	Regulatory Penalties	Serious Supply Chain	Serious Supply Chain	Management Failure
8	CNI State Sponsored Attack	Serious Supply Chain	Misuse of Data	Wildfires	Ethics and Trust
9	Wildfires	Misuse of Data	Theft of Proprietary Data	Misuse of Data	Regulatory Penalties
10	Serious Supply Chain	Wildfires	Social Media Attack	Social Media Attack	Serious Supply Chain

year in north-western parts of the U.S. and Indonesia.

Supply chain concerns appear in all top 10 figures for the first time. However, civil unrest and protest do not. Given the level of social protests in 2020 plus the pro-democracy demonstrations in Hong Kong and elsewhere, combined with a high-degree of public anger over the handling of Covid-19 in some countries, a higher rating may have been expected.

Figure 12: Business Sector — Risk Priorities

En	Banking Business Services (including consultancy) Energy and Utilities Pharmaceuticals Transportation and Logistics
Op	Education Financial Services and Brokerage Insurance
P	Government Public Sector Non Profit Retail
S	Engineering General Healthcare Hospitals Manufacturing Media and Entertainment Oil and Gas
T	Aviation/Aerospace Technology Telecoms

T Technology   Op Economic   S Social   En Environment   P Political

Climate change as an overarching resilience issue again failed to make any progress in our survey, despite the definition being clarified this year to be more relevant to business disruption factors. However, weather-related risks that are partly driven by climate change score reasonably well in most regions.

Sector Analysis

There were a total of 21 sectors recorded by survey participants. The general global risk categories were utilized to get an overall view of how sector's main priorities vary. For each of the 21 listed sectors, the most important global risk factor was:

Sector resilience concerns

The top seven sectors contributed over 70% of the results. They are:

1. Business Services
2. Banking
3. Insurance
4. Government
5. Hospitals
6. Manufacturing
7. Technology

Figure 13: The table below shows the top five PROBABILITY issues for each of these seven sectors

Sector	Probability 1	Probability 2	Probability 3	Probability 4	Probability 5
Business Services	Pandemic	Economic Failure	Operational Incidents	IT Long-term Outages	Misuse of Data
Banking	Pandemic	Operational Incidents	Economic Failure	IT Long-term Outages	Civil Unrest, Protests
Insurance	Pandemic	Severe Weather Events	Operational Incidents	Wildfires	Regulatory Penalties
Government	Pandemic	Operational Incidents	Severe Weather Events	Civil Unrest, Protests	Wildfires
Hospitals	Pandemic	Severe Weather Events	Serious Supply Chain	IT Long-term Outages	Civil Unrest, Protests
Manufacturing	Pandemic	Serious Supply Chain	Operational Incidents	Severe Weather Events	Wildfires
Technology	Pandemic	IT Long-term Outages	Severe Weather Events	Wildfires	Theft of Proprietary Data

Figure 14: The table below shows the top five IMPACT issues for each of these seven sectors

Sector	Probability 1	Probability 2	Probability 3	Probability 4	Probability 5
Business Services	Misuse of Data	Economic Failure	IT Long-term Outages	Operational Incidents	Pandemic
Banking	IT Long-term Outages	Theft of Proprietary Data	Misuse of Data	Pandemic	CNI State Sponsored Attack
Insurance	Regulatory Penalties	Economic Failure	Management Failure	Misuse of Data	Pandemic
Government	Pandemic	Operational Incidents	IT Long-term Outages	Terrorism	CNI State Sponsored Attack
Hospitals	Pandemic	Serious Supply Chain	IT Long-term Outages	Severe Weather Events	Economic Failure
Manufacturing	Serious Supply Chain	Operational Incidents	Pandemic	Severe Weather Events	Regulatory Penalties
Technology	IT Long-term Outages	Misuse of Data	CNI State Sponsored Attack	Operational Incidents	Theft of Proprietary Data

At a sector level, pandemics only top the resilience index for three of the seven sectors considered. These are insurance, government, and hospitals. However, it does appear in the top three for all sectors highlighted. In the 2019 report, pandemics appeared in most probability top 10 issues but never in the top 10 impact ratings. It is difficult to believe how different a society we were only a year ago.

Resilience priorities are still very sector-specific although this has been blurred in 2020 by the shared need to deal with the pandemic. There are also shared systemic risks, such as IT failure and extreme weather problems that affect every business. However, different sectors have different levels of concern; examples are data privacy and the economy in business services, regulation in insurance, technology in banking, supply chain in manufacturing and critical national infrastructure in high technology.

Clearly, sectors like air travel and hospitality face an existential crisis brought about by lockdowns and other restrictions placed upon them in attempts to suppress the spread of Covid-19. These are not businesses that can be run by people working for home and 2021 might prove terminal from some of them.

Impact of Regulation

Across the survey, 59.7% of respondents came from regulated firms and 40.3% from non-regulated firms. This shows a slight improvement in responses from non-regulated organizations over previous years (2019 had 38.2% non-regulated responses). This is not surprising, as it is known that regulated firms traditionally are more likely to have a formal resilience program in place, but other unregulated businesses are starting to see the benefits of such initiatives. The survey compared how regulated and non-regulated firms view the risks they face.

Figure 15: On the resilience index basis the following are the top 10 issues for each of the 7 sectors

Resilience Index Rating	Business Services	Banking	Insurance	Government	Hospitals	Manufacturing	Technology
1	Economic Failure	IT Long-term Outages	Pandemic	Pandemic	Pandemic	Serious Supply Chain	IT Long-term Outages
2	Misuse of Data	Pandemic	Regulatory Penalties	Operational Incidents	Serious Supply Chain	Operational Incidents	Misuse of Data
3	Pandemic	Operational Incidents	Economic Failure	IT Long-term Outages	IT Long-term Outages	Pandemic	Pandemic
4	IT Long-term Outages	Theft of Proprietary Data	Operational Incidents	Severe Weather Events	Severe Weather Events	Severe Weather Events	CNI State Sponsored Attack
5	Operational Incidents	Economic Failure	Misuse of Data	Terrorism	Economic Failure	Regulatory Penalties	Operational Incidents
6	Theft of Proprietary Data	Civil Unrest, Protests	IT Long-term Outages	Civil Unrest, Protests	Civil Unrest, Protests	IT Long-term Outages	Theft of Proprietary Data
7	CNI State Sponsored Attack	Misuse of Data	Severe Weather Events	CNI State Sponsored Attack	Terrorism	Theft of Proprietary Data	Management Failure
8	Management Failure	CNI State Sponsored Attack	Management Failure	Misuse of Data	Misuse of Data	CNI State Sponsored Attack	Severe Weather Events
9	Terrorism	Regulatory Penalties	Theft of Proprietary Data	Theft of Proprietary Data	Management Failure	Misuse of Data	Terrorism
10	Civil Unrest, Protests	Severe Weather Events	Wildfires	Wildfires	Theft of Proprietary Data	Economic Failure	Wildfires

Figure 16: Top five PROBABILITY ratings for both categories

Group	Probability 1	Probability 2	Probability 3	Probability 4	Probability 5
Regulated Firms	Pandemic	Operational Incidents	Severe Weather Events	IT Long-term Outages	Wildfires
Non-regulated firms	Pandemic	Economic Failure	Operational Incidents	IT Long-term Outages	Severe Weather Events

Figure 17: Top five IMPACT ratings for both categories

Group	Probability 1	Probability 2	Probability 3	Probability 4	Probability 5
Regulated Firms	Pandemic	Operational Incidents	Severe Weather Events	IT Long-term Outages	Wildfires
Non-regulated firms	Pandemic	Economic Failure	Operational Incidents	IT Long-term Outages	Severe Weather Events

The table below shows the top five PROBABILITY ratings for both categories (see figure 16, page 19).

The table below shows the top five IMPACT ratings for both categories (see figure 17, page 20).

The differences are relatively minor, both groups see pandemics are the most probable issue they have to deal with but extended IT outages are seen as potentially having the highest impact. Attacks on national infrastructure are of more concern to regulated firms as they are likely to provide support to government, while economic recovery is a much higher concern to non-regulated firms.

In previous surveys, questions have been asked which look at the extent to which respondents have had confidence in their senior management to handle a crisis successfully. Generally, this showed a higher degree of confidence across regulated firms than elsewhere. Naturally, for most respondents in earlier years, this was a largely theoretical perception as few executives had experienced a major business disaster or interruption.

In 2020, every organization was challenged, and every leadership team put under extensive stress to lead their companies through the Covid-19 crisis. Views this year are likely to be much more accurate and valuable. Performance during the crisis is a key observation, and the high level of concern about the potential for management failure in a crisis has not been confirmed. The good news is that senior management appear to have performed better when faced with a real challenge than many of their subordinates expected. Consequently, the issue of management failure in a crisis was number 5 in 2019 but has fallen to number 13 in 2020.

If we look at regulated and non-regulated firms in this context, there are many similarities but one important difference. The probability of future poor performance by senior managers is largely consistent with virtually no difference between the two groups. However, on the impact scale the problems poor crisis management would create is much higher for the non-regulated firms. One probable explanation for this factor is that regulated firms are likely to have a resilience program in place that can compensate to some extent for poor decision making at the time of crisis. Non-regulated firms are less likely to have this framework and are likely to be more dependent on good decision making at the time.

The role of the resilience professional

For each of the 20 key risk issues (see Figure 18, page 21), the survey asked resilience professionals to score: 1 – (not covered at all in the organization), 2 (done in organization but not by a resilience function), 3 (lead by other functions but with strong participation from resilience professionals), 4 (lead by resilience professionals but with support from other functions), and 5 (done entirely by the resilience professionals).

Scores of 1 clearly show a serious organizational weakness. Scores of 2 suggest the resilience professional's role is too limited, but conversely a score of 5 indicates an organizational failure to fully integrate and embed resilience. The ideal response would be 3 or 4 (involvement but working jointly to achieve solutions with others). It seems reasonable that a 3 score would work well for specialist issues like IT disruption, data security breaches, terrorism or social media attack and 4 would be appropriate for major operational disasters, extreme weather events, and pandemics.

The good news from this analysis is that for traditional continuity issues, the majority of survey participants give the ideal response. The resilience function has the major responsibility for the planning and preparation against pandemics, major operational incidents, and severe weather related incidents (all types).

For continuity issues where there is another specialist skill-set involved, the majority of survey participants also gave the ideal responses. The resilience function has a significant level of responsibility for mitigating IT long-term outages, serious supply chain disruptions, civil unrest and protests, crisis management failures, and terrorism.

For more abstract resilience issues where there is clear technical business leadership in another function, the majority of survey participants is not directly involved. While a significant number are involved in a supporting role, ideally, the level of participation should be higher for theft of proprietary data, misuse of private and corporate data, and social media targeted attacks.

For more strategic and emerging risk issues, there is very little participation from survey respondents in their organization's planning. In some cases, respondents indicate this is not being undertaken at all by any function – but this could be because such work is confidential and not widely disseminated to staff. These issues are: hostile state sponsored attacks on national or corporate infrastructure, the risk of unstable political regimes, social trends leading to concentration of risk in mega-cities, and lack of trust in the ethics behind new technology such as AI. It is unlikely that these items would be covered in many organizations' current appreciation of a resilience function. However, as the concept of a Chief Resilience Officer becomes more widespread, more strategic issues of this nature are likely to become part of the expanded role.

Figure 18: The level of involvement of the resilience professional in dealing with key resilience issues

Resilience ranking	Issue
1	Pandemic
2	IT Long-term Outages
3	Major Operational Incidents
4	Economic Failure
5	CNI State Attack
6	Theft of Proprietary Data
7	Severe Weather Events
8	Serious Supply Chain
9	Misuse of Data
10	Wildfires
11	Civil Unrest, Protests
12	Social Media Attack
13	Management Failure
14	Terrorism
15	Political Leadership Failure
16	Seismic Incidents
17	Concentration of Risk
18	Regulatory Penalties
19	Climate Change
20	Ethics and Trust

Reporting and business relationships

In 2019, this report defined the core disciplines that made up resilience management:

- Business Continuity
- Disaster Recovery
- Crisis Management
- Emergency Management

Other disciplines which are also components of a resilient organization are:

- Risk Management
- Information and Cyber Security
- Physical Security
- Compliance and Internal Audit

Other functional areas which might have resilience professionals embedded include:

- Information Technology (IT) and Telecoms
- Facilities Management
- Human Resources
- Procurement and Logistics
- Legal

The survey respondents defined the name of their current department as:

Department	Percentage
Business Continuity	36.40%
Resilience Management	14.91%
Risk Management	12.28%
Emergency Management	9.21%
Information Technology	7.46%
Crisis Management	5.26%
Compliance, Legal or Audit	4.39%
Information Security	3.51%
Physical Security	2.25%
Facilities Management	2.19%
Other Business Areas	2.13%

The use of the departmental name “resilience” has increased from 10.4% in 2019 to 14.9% in 2020. This is a significant increase and confirms a trend we identified in 2019. It suggests that resilience management is now being promoted and accepted as a legitimate business function. It is expected that resilience management will gain traction as an overarching term at a corporate level and, therefore, with HR departments. This will lead to more consistency in job roles across organizations, sectors, and regions.

In recent surveys, we attempted to evaluate the status of resilience professionals by analyzing their job levels and the levels of the individuals they report to. Given the range of titles and the large differences in company size, some degree of care needs to be taken in interpretation.

Levels were defined as:

Typical titles	Respondent	Manager
Owner, Partner, President	3.02%	10.77%
C-Suite Executive	4.12%	25.13%
Vice President	4.26%	12.82%
Director	13.76%	38.46%
Manager	36.58%	12.82%
Practitioner	38.26%	0.00%

The results are based entirely upon the titles provided in the survey. Respondents who did not indicate manager or above are listed as practitioners. A practitioner might be listed as team leader, project leader, or section head; roles which would probably be classified as managers in many organizations. While the split between manager and practitioner is not very precise, it is clear that over 75% of respondents fell into one of these two categories.

The most typical level for respondents' bosses is a director, and over 87% of respondents claimed to report to a director or someone more senior. This is a significant increase since 2019 when this percentage was only 67%. Again, care needs to be taken in interpretation as small specialist organizations will have different reporting levels than large-scale businesses. However, the technique used for analysis was consistent with previous years, so it does suggest that resilience as a profession is increasingly being recognized as important. In future surveys, we will collect data about organizational size so we can review how reporting varies with different types and sizes of organization.

Levels of professional certification

The professionalism of the resilience community can be indicated by the importance of professional certification. While the majority of survey respondents hold DRI certification, it is also useful to monitor those who hold certifications from other professional bodies and in related fields such as risk management, information security, project management, and audit. Across the entire survey, the following results were observed.

Category	Percentage
DRI Certification only	18.1%
DRI Certification and others	37.5%
Other Certification	26.3%
No Certification Held	18.1%

In North America, the following pattern was observed.

Category	Percentage
DRI Certification only	23.8%
DRI Certification and others	42.9%
Other Certification	18.8%
No Certification Held	15.5%

In other regions, the percentages for certified against non-certified were similar. Minor variations were seen with both Asian regions scoring higher than average and Europe and Latin America scoring slightly lower. DRI certification was highest in the United States, followed (in order) by Far East, Latin America, Middle East, and Europe. Other professional qualifications varied from region to region – some, like DRI, were internationally recognized, others more localised.

The DRI Future Vision Committee

Bringing together a global community of subject matter experts, DRI International has convened the Future Vision Committee, the leading global think tank on matters of operational resilience, discipline integration, and the future role of resilience professionals. This interdisciplinary group seeks to unite the profession by establishing meaningful and productive links among other professional bodies, higher education, and membership organizations.

Lyndon Bird is chair of the DRI Future Vision Committee. He has worked exclusively in business continuity since 1986 as a consultant, presenter, educator, author, and business manager. He has spoken at and chaired conferences throughout the world and has contributed features, articles and interviews to most leading business and specialist publications. He has been interviewed by a wide range of broadcasters, including the BBC, Sky News, Bloomberg TV and CNBC on continuity and resilience topics. Bird helped found the Business Continuity Institute in 1994 to promote and develop the emerging BC discipline as a professional field of activity and was a member of the original BS25999 Technical Committee. He was voted BCM Consultant of the Year in 2002 and given the BCM Lifetime Award in 2004 by Continuity, Insurance & Risk Magazine. He is currently Editor of the Journal of Business Continuity and Emergency Planning published in the UK and the US, an advisory board member for the US publication Disaster Resource Guide, and his new book “Operational Resilience in the Financial Sector” has recently been published by Incisive Media.

Patrick Alcantara has more than 10 years of experience in research, insight, and strategy. He currently leads future consumer trends work at Telefonica UK (O2), which feeds into innovation and proposition development. He is also former head of research and insight at the Business Continuity Institute (BCI) where he considerably extended the resilience industry’s evidence base. He has also managed research studies on behalf of organizations such as the former UK Department for Business, Innovation & Skills, PwC, BSI, SAP, and the World Health Organization. He is also a subject matter expert in resilience with 40+ publications and Editorial Board membership of 2 international peer-reviewed journals. He has also presented in various conferences including The European Information Security Summit (TEISS), International Disaster and Risk Conference (IRDC), ASIS Germany Conference, European Logistics & Supply Chain Conference, and the BCI World Conference & Exhibition.

Alcantara is from the Philippines and is currently based in the United Kingdom. He has a Diploma in Business Continuity Management, and a Bachelor’s degree in Psychology. He also attained a Master’s with Distinction from the Institute of Education (University College London) and Deusto University. He holds the Business Continuity Institute academic credential (DBCI) and is a member of the Market Research Society (MMRS), and the Future City and Community Resilience Network.

Linda Conrad is the principal of corporate and information security risk management at Exelon Corporation, a Fortune 100 Energy company. She is responsible for driving strategic risk activities and engagement with Enterprise Risk Management, Informational Technology, and the Chief Information Security Officer team. Conrad oversees cyber and physical security Key Risk Indicators and mitigation. Conrad is partnering with the National Institute of Standards and Technology (NIST) and Robert H. Smith School of Business on development and predictive analytics of the cyber supply chain risk portal, which received the 2017 Cybersecurity Award for Practice from Institute of Electrical and Electronics Engineers. Conrad served as interim chief executive officer of Climassure, where she led a team which pioneers innovative financial and technology products, data modeling, and advisory solutions to help mitigate the economic impacts of extreme weather and flooding. For 15 years prior, Conrad managed a global team responsible for delivering tactical solutions to Zurich Insurance and customers on strategic issues such as business resilience, cyber and supply chain risk, enterprise risk management, and total risk profiling.

Andrea Bonime-Blanc, JD/PhD, is CEO and Founder of GEC Risk Advisory and a global governance, risk, ESG, ethics, cyber and crisis strategist, serving business, nonprofits, and government. Since 2017, she has served as the Independent Ethics Advisor to the Financial Oversight and Management Board for Puerto Rico. She serves on several Boards and Advisory Boards including Greenward Partners (a Spanish green energy firm), Ethical Intelligence (an EU-based AI ethics firm), ProtectedBy.AI (a US based AI cybersecurity firm), Epic Theatre Ensemble (a NYC nonprofit), the NACD New Jersey Chapter and NYU Stern-based think tank, Ethical Systems. She serves as a Governance Mentor at Plug & Play Tech Centre, a global start-up eco-system, is a NACD Board Leadership Fellow and Governance faculty and holds the Carnegie Mellon CERT Certification in Cyber-Risk Oversight. She is a life member of the Council on Foreign Relations.

Andrea spent two decades as a c-suite global corporate executive at Bertelsmann, Verint, and PSEG overseeing legal, governance, risk, ethics, CSR, compliance, audit, InfoSec and environmental health and safety. She began her career as an international corporate lawyer at Cleary Gottlieb.

Andrea is a global keynote speaker and graduate faculty at NYU teaching “Cyber-Leadership, Risk & Resilience”. She is an extensively published author of many articles and several books including The Reputation Risk Handbook, Emerging Practices in Cyber-Risk Governance and The Artificial Intelligence Imperative. Her latest book, Gloom to Boom: How Leaders Transform Risk into Resilience and Value (Routledge 2020) debuted as an Amazon #1 Hot Release in Business Ethics and Game Theory. She was born and raised in Europe, is multi-lingual and received her joint Juris Doctor and PhD in Political Science from Columbia University. She lives in New York City with her family and is an avid photographer and artist.

Boris Issavi is the director of business continuity management at Global Payments Inc., where he oversees the enterprise-wide BC and DR operations across the organization’s global footprint. He has systematically built his expertise in operational risk over the past 20 years. For almost 10 of those years, he has been dedicated to business continuity and disaster recovery with global companies in the financial industry. In his current role, Issavi manages all phases of planning, analysis and implementation of technical solutions in direct support of resiliency and information security objectives from the conceptual stage to the final execution. As a leader, he works to create an environment where ideas can flourish and effective solutions materialize.

Richard Knowlton is chairman of Knowlton Associates and is a member of the Cyber Resilience Advisory Board of the Digital Leaders’ Forum, an Associate Director of Strategia-Worldwide and an honorary Life Member of the International Security Management Association (ISMA). Knowlton was Group Corporate Security Director of Vodafone (2009-2015), after previously working in Milan as Head of Security (Global Operations) for the Italian UniCredit Group, the largest bank in Central and Eastern Europe. Between 2014-2017, Knowlton was Executive Director (Europe) of the non-profit Internet Security Alliance (ISA), a multi-sector trade association based in Washington DC. He was also previously a board member of the Commonwealth Cyber Crime Consortium and of the UK government’s Overseas Security Information for Business (OSIB).

Knowlton has spoken extensively on digital security risk management on the BBC and regularly presents at major international events, such as the Mobile

World Congress in Barcelona (2017-2018). He is the three-times chairman of the Security of Things World Conferences in Berlin (2016-2018). Richard worked in the UK Foreign Service before entering the corporate sector. He is based in Italy.

David Porter has been the director of business continuity management at the Australian Taxation Office (ATO) since 2010. He has also chaired a whole-of-government BCM Community of Practice, with members from over 35 Commonwealth and state based agencies. Porter and his team provide regular mentoring support for other organizations and have contributed towards readiness activities across the public sector and wider finance industries. Porter is a regular presenter at industry events and contributor to the Oceania 2020 think-tank. The ATO BCM team has won the Australasian Business Continuity Institute Team of the Year award three times and the team's integrated BCM Framework and approach to organizational resilience have also been recognized in two peak Australian Government insurer awards for excellence in risk management.

Richard Reed leads the crisis and continuity management efforts for Saudi Aramco, the state-owned oil company of the Kingdom of Saudi Arabia and a fully-integrated, global petroleum and chemicals enterprise with the world's largest spare crude oil production capacity and crude oil reserves. Reed was previously senior vice president of disaster cycle services at the American Red Cross. In this role, he led the development and execution of programs that help Americans prevent, prepare for, and respond to disasters nationwide. Prior to the Red Cross, Reed was at the White House, serving as deputy assistant to the president for homeland security. He led the development of national policy related to resilience, transborder security, and community partnerships. With an experienced team of over 30 senior professionals, Reed covered a broad and deep homeland security portfolio that includes all-hazards preparedness, individual and community partnerships and resilience, critical infrastructure protection and resilience, domestic incident management, continuity of government, national exercises, transportation security (aviation, maritime, and ground), piracy, information sharing, border security, and immigration. Reed's prior White House tenure included service as special assistant to the president for homeland security and director for continuity (2006-2009) and special assistant to the president and senior director for resilience policy (2009-12). Reed's federal service exceeds 20 years, with positions in the Department of Veterans Affairs, the Federal Emergency Management Agency, and the General Services Administration.

Wolfgang Mahr has over 20 years of experience in consulting and project management in the ICT environment and over the last 15 years has specialized in the field of business continuity management. He is experienced in IT governance, information security, business management, marketing, account and product management, in professional education as an author of educational content and international speaker. He holds a PhD from the Swiss Federal Institute of Technology in Lausanne (EPFL), has earned a Bachelor of Business Administration degree from GSBA Zurich, is a Certified Information Systems Auditor (CISA) and is a long-time member of the Business Continuity Institute (MBCI). His professional publications, blogs, and lectures at international conferences support the exchange of ideas and further development of current BCM issues. He participates in global standards bodies (ISO TC 292, CEN TC 391) and is a past President of BCMnet.CH. He is fluent in German, English, and French.

Kenji Watanabe is a professor at the graduate school of engineering, and also the head of disaster and safety management of the Nagoya Institute of Technology, with major research areas in risk management, business continuity management, and critical infrastructure protection. He has almost 20 years of business experience at the Mizuho Bank and PricewaterhouseCoopers in financial business and risk management fields.

About DRI International

Disaster Recovery Institute International (DRI) is the oldest and largest nonprofit that helps organizations around the world prepare for and recover from disasters by providing education, accreditation, and thought leadership in business continuity, disaster recovery, cyber resilience and related fields. Founded in 1988, DRI has certified 15,000+ resilience professionals in 100+ countries and at 95 percent of Fortune 100 companies. DRI offers 15 individual certifications, including the globally-recognized CBCP certification, and certifies organizations as resilient enterprises. DRI offers training programs ranging from introductory to masters level across a variety of specialties in multiple languages; online and in-person continuing education opportunities; and an annual conference dedicated to the resilience profession. DRI supports charitable activities through the DRI Foundation.

DRI provides independent analysis and standard-neutral, technical advice for governments and international organizations as the voice of the resilience profession. DRI is a Standards Development Organization accredited by the American National Standards Institute (ANSI), an International Organization Liaison Observer to the International Organization for Standardization (ISO) Technical Committee 292 that manages ISO 22301, a CQI and IRCA Approved Training Partner, a National Initiative for Cybersecurity Careers and Studies (NICCS) Training Provider, and a United Nations Office for Disaster Risk Reduction ARISE Initiative Partner. Our certification programs are recognized by various government agencies including the U.S. Federal Government via the Montgomery GI Bill and the GSA Schedule.

From our inception, we have and continue to advocate an inclusive environment that enables everyone to develop their skills and make a difference through education and accreditation. Diversity, inclusiveness, and the promotion of mutual respect is exemplified in all facets of our goals and mission, including the Board of Directors’ membership, staff, thought leadership and charitable activities worldwide.

For more information, visit our website or contact a representative today.
drii.org | (866) 542-3744 | info@drii.org