The Third Annual DRI International Global Risk And Resilience Trends Report

Thought leadership for the profession by the profession

Executive summary

Published each November, the DRI International Global Risk and Resilience Trends Report is essential reading for resilience professionals. It provides a summary of key trends that emerged over the course of the year as well as insight into the current state of the profession. The report is developed by DRI International's Future Vision Committee, which is comprised of a team of international thought leaders and experts (see Future Vision Committee Year in Review, page 4). This year, the report also is supported by the views of a wide range of certified business continuity practitioners who were surveyed on a variety of issues (see Survey Results, page 9).

The report concentrates on those areas where operational resilience can be improved by the adoption of best practices. A key feature is an assessment of current resilience practice and how it can become increasingly effective. Furthermore, the report suggests ways in which resilience professionals can make the greatest contribution to the continuation and success of their organizations.

Providing evidence-based analysis of risks that concern all organizations, this report also shows how resilience professionals view those risks. Additionally, it offers much more, addressing contentious issues that are written about in journals and presented at conferences – with great frequency but often with little proven validity. Such issues include:

- Do resilience professionals struggle to make their case on issues that are traditionally not viewed as Information Technology/Disaster Recovery (IT/DR) related?
- To what extent is business continuity a tool to help manage cyber threats?
- Are supply chain failures now a priority resilience issue for global businesses?
- Do financial services organizations have more resilience expertise than those in other sectors?
- Are the resilience concerns of different regions of the world consistent or starting to diverge?

The insights presented here have great value not only to resilience professionals, but also to those working in related fields, such as risk management, emergency management and information security.

Overview

In last year's trends report, the top three resilience issues all were technology based – the business consequences of major IT failures, cyber threats in various guises, and inadequate investment in information security and resilience. These issues continue to perform strongly as potential risks, but there is now an even greater acceptance by management that failure to manage them effectively would be harmful or even business-fatal.

All organizations understand that some technology interruptions are probably inevitable and will have an impact on their ability to trade as normal. Business continuity and the other resilience-related disciplines are becoming strategic issues in corporate thinking – although the practices adopted are still mainly tactical and operational. This gap must be addressed.

This year, our survey reveals other interesting findings concerning the responsibilities of today's resilience professional. Far from simply being IT/DR specialists, many are looking at the implications of diverse national and international risks. It seems that most organizations have accepted that good business practice and security only partially can protect them against myriad random incidents. They recognize that they must mitigate residual risk by having rigorous response plans and viable recovery strategies in place.

Areas where resilience professionals are starting to bring their planning and exercising skills to bear include:

- The operational consequences of supply chain disruption
- Flooding and other extreme weather events
- Reputational damage from social media and other online attacks
- Compliance failure, with respect to data protection and privacy legislation
- Pandemic planning and other health-related risks

We have, however, seen one area to which significant attention has been drawn in 2017 – the question of cyber as an existential threat to our accepted way of life. A year ago, according to the World Economic Forum, the U.S. was the only major economy that viewed cyber as the greatest threat to its continued success. Within a year, this has changed to include virtually the entire world. Certified resilience professionals share this view; a large number consider cyber risk the biggest problem their organizations face. However, while many resilience professionals are involved in this activity within their organizations, even more are not. More than 50 percent of those surveyed felt that they had no or very little direct involvement with planning response measures for cyber breaches. This apparent dichotomy will be discussed later in this report.

Note

DRI International does not take political positions or advance political causes of any kind.

DRI International reserves the right to reference instability or uncertainty caused by events – political or otherwise – only insofar as the repercussions of those events may have an impact on the resilience field and the ability for organizations to prepare for and recover from them.

The Top 8 Global Risk and Resilience Trends

The following trends are provided as helpful guidance for those professionals tasked with managing business continuity, organizational resilience or similar functions within their companies or other places of work. When the words "resilience professional" are used below, they generally refer to those who are qualified practitioners in fields which are covered by the DRI Professional Practices for Business Continuity Management.

1. The core role of resilience professionals remains the management of situations which could best be described as "disruptive risk."

Organizations focus their professional input on concrete risks, such as IT failure and major incident response. The key criteria for determining if a situation is within that remit still appears, in many cases, to be restricted to known operational interruptions. Senior management still tends not to solicit specialist opinion from resilience professionals about the consequences of strategic issues that are not normally associated with disaster recovery or business continuity.

2. Resilience professionals have a clear vision about the relative importance of a wide range of risks to their organization's continuity, or even its survival.

However, they are not always able to have sufficient involvement in the decisions about how that risk could be better managed. The most obvious example is cyber (in its widest context) where almost 40 percent of those surveyed have no involvement in planning business responses to such threats. In fact, if we include a minor involvement, more than 50 percent of resilience professionals are largely excluded from helping to mitigate their organization's largest risk.

3. Supply chain disruptions are increasingly perceived as a significant business risk for large, complex organizations.

Globalization and the risk of supply interruption as a result of civil conflicts, extreme weather incidents, or transportation failure are identified as possible causes. However, the ability to guarantee a reliable supply chain is also a major issue for domestic companies in sectors such as energy and healthcare. The involvement of resilience professionals in this area has broadened, although their role still tends to be handling the consequence of supply failure rather than incorporating embedded resilience in the supply chain.

4. The resilience profession has broadened and matured significantly, with responses to our survey being fielded from almost every business sector imaginable.

The financial sector still has the largest number of participants, but at only 27 percent of all respondents, it does not distort the overall figures. However, the breadth of participation in a wide range of corporate risk issues still seems higher in finance than in other sectors. This might be due to the regulated nature of finance, where all risks have to be assessed, appropriate controls put in place and compliance proven. In non-regulated industries, a less comprehensive risk management structure might be in place, thus giving less opportunity for participation.

5. Our analysis shows very little difference in the views and opinions of resilience professionals globally when it comes to identifying the risks about which they are most concerned.

Concerns about technology failure were slightly higher in Europe than elsewhere, whereas in North America and Asia all rankings were virtually identical. We conclude that globalization has created a more homogeneous resilience community across the major trading regions of the world. Political leaders might express widely different policies, but at a business level, we all seem to be dealing with the same resilience challenges and using much the same methods and techniques.

6. Crisis management skills and techniques are being incorporated into the traditional business continuity landscape.

This development has widened the remit of some resilience professionals to allow them to participate more fully in planning for crises, such as a financial shocks, regulatory non-compliance and social media hostilities. This trend is still at an early stage in many organizations, but it is evolving.

Many business continuity professionals consider cyber risk the biggest problem their organizations face. However, more than 50 percent of those surveyed felt that they had no or very little direct involvement with planning response measures for cyber breaches.

7. There has been less progress than expected in bringing together various related disciplines under one coherent resilience portfolio.

The initiative from The Rockefeller Foundation called 100 Resilient Cities has created a role called Chief Resilience Officer which is funded by the foundation. However, this has not spread widely to the commercial sector. The once apparent inevitability of risk management, business continuity, and information security merging has not materialized to any significant degree. Other studies that have focused on breaking down functional silos have suggested that various disciplines already mentioned (plus insurance, emergency management, and physical security) are communicating more than in the past. However, we are a long way from the acceptance of a common, overarching resilience management discipline.

8. There are still too many organizations where resilience professionals are seen (and also see themselves) just as the people who know what to do when things go wrong.

They should also be viewed as the people who help prevent things from going wrong in the first place. A good understanding of corporate strategy, risk appetites, and C-level business concerns is essential for resilience professionals. One way of gaining this knowledge is by persuading top-level managers to participate in workshops which address their business interruption concerns. Too often, opportunities for dialogue are lost when the only questions that top executives are asked at exercises are about dealing with emergency evacuation.

The DRI Future Vision Committee Year In Review

Our findings are based on the research and opinions of a range of highly experienced professionals who make up the DRI International Future Vision Committee (To learn more about the Future Vision Committee and its members, visit https://drii.org/about/futurevision). The knowledge of the committee is supplemented with an extensive review of expert opinion from published sources, such as the World Economic Forum (WEF), the Organisation for Economic Co-operation and Development (OECD), and the International Monetary Fund (IMF). What follows is a summary of those findings by topic:

Global Politics

On a global political scale, the growing nuclear ambitions of North Korea resulted in the U.S. having to dedicate increased focus to this potential area of conflict. The ramifications of failure in resolving this stand-off could hardly be more serious for the world. A North Korean strike on a U.S. ally or military base could trigger a war in which all the major powers are engaged. Most geopolitical experts do not think it will happen, but world military tension is at the highest level since the end of the cold war.

The war in Yemen has led to some of the worst humanitarian crises in modern times, with the major powers unable to influence what is essentially a proxy struggle for strategic influence and control by key players in the region. The scale of the humanitarian crisis in Yemen and the alleged ethnic cleansing and mass migration of the Rohingya people from Myanmar to Bangladesh were among the worst such incidents we have seen in many years.

In Latin America, there are varying patterns emerging. On the negative side, chaos continues in Venezuela, where the people of an oil rich state live in abject poverty. The government is unable to feed or medically treat its population or provide even the most basic infrastructure support. However, one positive development for the region was the signing of the Colombian peace deal between the government and the Revolutionary Armed Forces of Colombia (FARC) rebel group. This armed conflict has lasted 52 years and the deal is seen as highly significant for the future success of the country.

Much of the African continent seems to be facing severe difficulties as well. Even South Africa might be turning away from the rainbow nation vision of Nelson Mandela as African National Congress (ANC) leaders lose popularity following many recent scandals. Kenya also faces widespread political unrest and extensive popular insurgency, with the result of its presidential election annulled by its own courts. Nigeria, which is Africa's most populated country, struggles to deal with widespread terrorist activity and international concerns about corruption. Civil war, famine, and ethnic cleansing threaten a number of countries and the next migration crisis facing Europe might well come from Africa.

After many years of largely consensus-based politics in Europe, there now appears to be a much wider ideological gap between parties of the right and the left across many countries. Although the far-right parties in the Netherlands, Austria, France, and Germany had no outright successes, they did gain votes and more seats in their respective parliaments. This is particularly interesting in Germany where Chancellor Angela Merkel's hold on power is weaker than it has ever been before.

The arguments for independence, new nation states, and distrust of entrenched political establishments have continued. Although Brexit negotiations are progressing very slowly (as we predicted last year), they are not likely to challenge the established

rule of law whatever the final outcome. Potentially, more damaging to European unity is the unilateral declaration of independence by Catalonia and Spain's response. This is an ongoing crisis as of the time of writing this report, but positions are so far apart that it is unlikely to be resolved quickly or totally peacefully.

After a bad 2016, the European Union stabilized to some extent both economically and politically. As the Brexit separation date approaches and the implications to both the UK and EU economies starts to become clearer, this could change. The value of the Euro, and the improved growth in parts of the Eurozone, largely have been generated by extensive quantitative easing from the European Central Bank. When global interest rates start to rise again, we could see another Euro crisis in the not too distant future. French President Emmanuel Macron has provided a radical blue-print for a fully integrated political union, but this is unlikely to find much favor in France and certainly none in former Eastern Bloc countries, such as Poland and Hungary.

Terrorism and Extreme Violence

International terrorism remains a major issue. Although ISIS will soon be defeated militarily in Syria and Iraq, its ideology has not been erased and attacks will continue on a global basis through other means. Our assessment last year was that future attacks would be on a smaller scale, not directed at heavily policed targets, and more likely to be random assaults requiring little coordination. This proved true, with the weapon of choice often being a passenger car or commercial vehicle. Between 2000 and 2015 there were a total of 31 reported vehicle ramming attacks across the world (an average of fewer than two per year). Since last year's report, there have been 27 such incidents – 11 of which resulted in multiple fatalities. While the highest profile incidents were in Berlin, London, Stockholm, and Barcelona, vehicle attacks also were reported in France, Germany, Unites States, Israel, and Canada.

In addition to vehicle ramming attacks, there have been many other terrorist attacks across the world. The suicide bombing by an ISIS-inspired supporter of a popular UK music venue in Manchester killed over 20 young music fans and received much international attention.

However, extreme violence is not restricted to international terrorism or terrorism at all in its conventional sense. In the U.S. the brutal murder of country music fans in Las Vegas in October left more than 50 people dead and 500 more injured. This demonstrates the unpredictable and dangerous nature of today's world. We may not always be able to understand what motivates killers, but we must be prepared to address the effects. To the person responding to an incident, they do not know if it is terrorist related or not – their priority is dealing with what has happened, not why.

Natural Disasters

The year 2017 also saw many natural disasters. We experienced an extremely active hurricane season and a number of other extreme weather events. Hurricanes Harvey, Irma, and Maria cutting across the Caribbean in unusually quick succession caused total destruction to some small countries as well as significant damage to wide parts of the U.S. Puerto Rico was especially badly affected by Maria. The small island's industry and infrastructure was effectively destroyed and, without it, the tourist trade will cease. The island faces financial ruin. It is now totally dependent upon financial and operational support from the U.S.

Natural disasters often punish the most vulnerable countries, as happened with the mud slides in Sierra Leone. This is a country battered by civil war, still recovering from Ebola, and then hit with a catastrophic natural disaster. Flooding took its usual toil in South East Asia but was particularly extreme across parts of India, Bangladesh, Nepal and Pakistan. Reports suggested over 40 million people were affected to some extent with at least 1,200 deaths.

Recently, two earthquakes in Mexico resulted in considerable loss of life and property. Although neither was as severe as the 1985 earthquake which killed 10,000 people in and around Mexico City, the fact that two earthquakes occurred within 12 days (the second was not an aftershock) was unusual.

Severe wildfires also were a strong feature in 2017, with extensive damage and loss of life in Spain and Portugal and the destruction of parts of the Northern Californian fine wine regions of Sonoma and Napa. There were also significant problems with wildfires in the Canadian province of British Columbia.

As resilience professionals, we can neither stop natural disasters nor change the fact that the most vulnerable are often the hardest hit. However, working with non-governmental organizations (NGOs), charities, and international organizations including the UN, we can help mitigate some of the worst suffering. In addition, we must be prepared to deal with the impacts such disasters have on our organizations, as our facilities may be destroyed, staff killed or made homeless, or our supply chains fatally interrupted.

Our competence and capabilities are likely to be tested mightily in the coming months and years. Even if our skill sets are adequate, we require the resources and support to deal with increasingly frequent severe extreme weather events.

Climate Change

There is no definitive evidence to suggest that any of these extreme weather events had any direct connection with climate change. However, given the current world-wide emphasis on environmental issues, many people do make the case for a link. There has been some international concern about the U.S. Administration's ongoing commitment to global environmental initiatives. However, since the U.S. is moving ahead with cleaner and greener energy sources and new technologies faster than any other major economy, on balance this is likely to create a mainly positive environmental impact.

Technology and Social Change

Technological change and the inherent risks it brings are of great interest to the resilience community. However, cyber and new technologies are widely accepted as one of the chief dangers to global stability. We must include within this overarching risk the dangers resulting from interconnection of these new technologies, which even The World Economic Forum described as our greatest "resilience challenge."

In fact, 2017 was probably the year when the general public began to fully appreciate that information security risks can impact them personally and directly. Allegations of Russian involvement in the U.S. presidential election set the tone for the year. Email hacks and "fake news" on the internet demonstrated the potential for such interference.

Information security is now so important that it cannot be considered just a technical speciality left to experts to resolve. Technical change is now happening at an unprecedented rate with the Internet of Things (IoT) becoming a reality in many homes and driverless cars being tested on active roadways in urban centers. Artificial intelligence and robotics are already changing the way business operates and leading to demands for increased regulation and government control. Some political parties in Europe have even suggested higher taxes on companies that use robots in order to encourage a return to manual working. Such ideas, although unsustainable and somewhat short-sighted, are finding favor with some of the electorate.

This concern is hardly surprising, as research suggests that 80 percent of U.S. job losses in the period 1997-2007 were due to new technologies. Although technology may generate jobs for those with high levels of education and technical skills, it is one of the main factors creating unsustainable levels of unemployment or under-employment in many parts of the world. According to the World Economic Forum, this leads to profound social instability and can result in moderate governance losing popular support.

Technology Vulnerability

During 2017, the business community often was reminded of its cyber vulnerability, with DDoS and ransomware attacks increasing in frequency (if not always in sophistication). On one occasion, the critically important National Health Service network in the UK was badly compromised by a virus known as "WannaCry". This virus affected organizations in around 150 countries and was eventually found to have probably originated in North Korea. Shortly afterwards, another ransomware virus coded "Petya" spread from Ukraine across EU countries, Russia and beyond. Governments and airports were affected as well as many multi-national firms with trading links to affected countries.

Perhaps the most serious cyber incident involving the public was the Equifax hack. In what has been described in the media as the worst corporate breach of security ever, the credit scoring and referencing giant was hacked, exposing 143 million people to possible identity theft or fraud. Equifax's share value plunged and legal cases are mounting. Other examples of commercial cyber activity included stolen new program content from U.S. broadcaster HBO and the penetration of the email system at the multi-national accounting and consulting firm Deloitte. Particularly embarrassing to Deloitte was the fact that they had been voted "best cybersecurity consultancy in the world" only two years earlier.

In a bizarre development, U.S. agencies discovered that Russian government spies, in an attempt to uncover U.S. military secrets, hacked anti-virus software produced by Kaspersky Lab (a Russian company); the software is widely used in the U.S. and by its allies. While the software was removed from all sensitive government computers, the incident raises questions about why that product was being used at all.

It is not only new technologies that are causing business continuity problems. Complex legacy and corporate systems also are prone to fail. A spectacular example was the total IT failure of British Airways during the May bank holiday weekend in the UK. No flights for virtually three days ruined holidays, weddings, business appointments, family reunions, and so on for some 75,000 travellers worldwide. It is expected to cost the airline up to £ 150m in compensation payments; damage to the airline's reputation is incalculable. The CEO of the parent company claimed that the reason was human error – a contractor had accidently disconnected a power cable and had reconnected it incorrectly. To a professional in the resilience field, this explanation does seem very unlikely. If our discipline cannot deal with a minor electrical fault without bringing a major airline to a complete halt for days then we really need to go back to the drawing board.

Business Challenges

It is not only British Airways that had a bad year in the airline business. An even more egregious example was United Airlines, which gave a masterclass in how not to manage a reputational crisis. Dragging a passenger who refused to change flights and had a valid seat assignment from the aircraft in full view of passengers live on social media (and hence national and international media as well) was bad enough. However, the incident was compounded by the CEO justifying the actions of his staff. Almost immediately, the impact on share price was felt with 4 percent wiped off the market value of the holding company. Although this recovered partially, the reputational damage was done and continues. Their slogan "flying the friendly skies" could not have seemed less apt.

Europe's largest carrier, Dublin based Ryanair, also had a disastrous year. It suddenly cancelled hundreds of flights with no notice – claiming it had insufficient pilots. It then allegedly failed to comply with generally accepted airline terms on alternate bookings and compensation. Not surprisingly, it faced a major media and social media storm.

The commercial success and failure of corporate entities as a result of market competition or poor management is typically beyond the scope of business continuity and organizational resilience. However, changes in technology are leading to a rethink of the viability of traditional, large retail operations, because as more and more purchasing is done on-line, the risks of technology failure and the use of cyber for theft, fraud, or blackmail increases rapidly. Wells Fargo, an iconic name in financial services, was fined $185 million by regulators for a cross selling fraud which was largely due to misuse of technology. Over 5,000 employees were dismissed following the investigation and the bank lost many of its most important clients.

The scale of household name brands in the U.S. alone that have struggled in 2017 is astounding. The business owning Macy's, the world's largest department store, shed 10,000 jobs over the past 18 months and is at risk of hostile take-over. The world's largest toy chain, Toys R Us, was forced into bankruptcy protection in the U.S. and Canada. Other iconic stores are suffering a similar fate; JC Penney is closing 138 U.S. locations and Sears is closing 178. Upmarket Neiman Marcus is closing almost a third of its outlets amid unsustainable levels of debt. At the smaller and more niche end of the market, similar troubles are occurring at Vitamin World (closing 51 of 334 stores) and Claire's Fashion Accessories, which is unlikely to survive beyond the end of 2017 according to Fitch ratings agency.

It is not only retail that struggled to keep pace with the changing technologies and customer expectations. Former Asian high-fliers like Taiwanese HTC Telecom, which produced the first ever Android phone in 2008, looks set for bankruptcy or a "fire-sale" takeover. Takata, the Japanese air-bag manufacturer, has had serious legal and reputational problems with product safety. This was highlighted in our report last year and the company went into bankruptcy in the U.S. during 2017.

Media and entertainment industries also suffered in 2017, with sexual harassment scandals emerging at Fox News and even more dramatically at The Weinstein Company. Organizations can no longer manage these incidents internally or sweep them under the rug, as these reports quickly become world news with a massive negative impact on brand and reputation.

Uber is perhaps the most surprising business to be hit with reputational problems. The epitome of the "gig-economy" and the modern way to provide on-demand services, the alternate taxi business is now banned in Italy and Denmark and coming under pressure in many countries for unethical business practices, failure to manage drivers, and indifference to complaints of sexual assault. Uber's largest market outside of the U.S. is London, and the London Transport Authorities refused to renew its licence. The company is also suffering from claims that it attempted to dupe regulators by using deliberately flawed software.

Survey Results

Although expert opinion is a key component, we also believe that experience from working practitioners who hold DRI professional certifications is of great value. Therefore, the committee identified 20 key risks and we asked DRI Certified Professionals for their thoughts on them from an organizational, industry-specific and regional perspective.

The key risks that were listed for consideration are shown in Figure 1 (page 11).

The survey asked three key questions about each of these 20 key risks:

1. What is the probability that the respondent's organization would be directly affected by this issue during the next 12 months? (Scale of 1 to 5, with 1 being the lowest and 5 the highest)

Business continuity and the other resilience-related disciplines are becoming strategic issues in corporate thinking – although the practices adopted are still mainly tactical and operational. This gap must be addressed.

2. What would the potential overall impact be on the organization's viability should this actually occur in the next 12 months? (Scale of 1 to 5, with 1 being the lowest and 5 the highest)

3. To what extent is the respondent as a resilience professional personally involved with this issue? (Scale of 1 to 5, with 1 being no involvement and 5 having total responsibility)

For questions 1 and 2, a simple statistical average was calculated (MEAN VALUE) with the corresponding rankings displayed in Figures 2 and 3 (page 12). To develop a "Resilience Risk Index," we multiplied the scores in Figures 2 and 3 (see Figure 4, page 13).

For question 3, interpretation of these results is not entirely straightforward. Rankings of 1 are clearly a poor result (indicating no involvement in the issue), but conversely a score of 5 indicates failure to achieve any buy-in across the organization. After consideration, the ideal response would be 3 (indicating a strong involvement of the resilience professional, but working jointly to achieve solutions with other affected functions). We looked for the response that occurred most frequently which in statistical terms is the MODE VALUE. We also calculated the MEDIAN VALUE (i.e. the middle number in the data set). Ideally both MODE and MEDIAN values would be 3. These results are shown in Figure 7 (page 14).

In addition, the survey aggregated these 20 items into 5 high-level global risks:

- Technology Failure (Cyber or IT malfunction)
- Supply Chain Failure (all potential causes)
- Political and Economic Instability
- Terrorism and Random Violence (domestic and international)
- National Infrastructure Failure (all potential causes)

This short list was used for reviewing high-level differences between regions and sectors. It used the percentage that voted for each category to determine the comparative importance placed upon each factor by respondents.

The top three resilience issues identified by respondents are major IT interruptions, natural disasters, and cyber-attacks. These are generally in line with the conclusions of studies such as the WEF Global Risk Survey.

Figure 1: List of 20 Key Risks Identified by FVC

Figure 2: The probability of the defined risk, threat or hazard causing organizational problems during 2018

Rank	Issue	Mean Value
1	Major IT interruption due to technical malfunction or human error	3.62
2	Criminal cyber attacks	3.05
3	Extreme natural disasters (earthquake, volcano, hurricane, tornado)	2.94
4	A global financial crash as severe as 2007/2008	2.92
5	Inadequate investment in information security	2.82
6	Severe reputational damage from targeted social media campaign	2.80
7	State-sponsored cyber attacks	2.77
8	Wide-scale flooding outside of manageable levels	2.70
9	Failure of critical national infrastructure in a major country	2.61
10	A man-made disaster to nuclear, chemical, gas, or oil facilities	2.59
11	Coordinated and organized terrorist attacks	2.55
12	Political unrest leading to government collapse and civil disturbance	2.49
13	Random attacks of extreme violence	2.48
14	Pandemic which spreads quickly with extensive global fatalities	2.47
15	Serious supply chain disruption causing significant financial loss	2.37
16	Non-compliance with privacy and data protection laws	2.34
17	CBRN (chemical, biological, radiological, nuclear) attack on a large city	2.23
18	A new cold war between East and West	2.17
19	Military conflict between U.S. and North Korea	2.15
20	Uncertainty over UK/EU Brexit negotiations	2.02

Figure 3: The impact on resilience if the defined risk, threat, or hazard actually happened during 2018

Rank	Issue	Mean Value
1	Major IT interruption due to technical malfunction or human error	3.53
2	A global financial crash as severe as 2007/2008	3.21
3	Extreme natural disasters (earthquake, volcano, hurricane, tornado)	3.21
4	Severe reputational damage from targeted social media campaign	3.12
5	Criminal cyber attacks	3.09
6	Inadequate investment in information security	3.06
7	State-sponsored cyber attacks	3.01
8	Pandemic which spreads quickly with extensive global fatalities	2.97
9	A man-made disaster to nuclear, chemical, gas, or oil facilities	2.95
10	Failure of critical national infrastructure in a major country	2.94
11	Non-compliance with privacy and data protection laws	2.94
12	Wide-scale flooding outside of manageable levels	2.88
13	Coordinated and organized terrorist attacks	2.87
14	Political unrest leading to government collapse and civil disturbance	2.83
15	Serious supply chain disruption causing significant financial loss	2.71
16	Random attacks of extreme violence	2.66
17	CBRN (chemical, biological, radiological, nuclear) attack on a large city	2.62
18	Military conflict between U.S. and North Korea	2.28
19	A new cold war between East and West	2.26
20	Uncertainty over UK/EU Brexit negotiations	2.06

Figure 4: The resilience risk index for 2018 based upon both likelihood and impact

Rank	Issue	PROB	IMP	Resilience Index
1	Major IT interruption due to technical malfunction or human error	3.62	3.53	12.78
2	Extreme natural disasters (earthquake, volcano, hurricane, tornado)	2.94	3.21	9.44
3	Criminal cyber attacks	3.05	3.09	9.42
4	A global financial crash as severe as 2007/2008	2.92	3.21	9.37
5	Severe reputational damage from targeted social media campaign	2.80	3.12	8.73
6	Inadequate investment in information security	2.82	3.06	8.63
7	State-sponsored cyber attacks	2.77	3.01	8.34
8	Wide-scale flooding outside of manageable levels	2.70	2.88	7.78
9	Failure of critical national infrastructure in a major country	2.61	2.94	7.67
10	A man-made disaster to nuclear, chemical, gas, or oil facilities	2.59	2.95	7.64
11	Pandemic which spreads quickly with extensive global fatalities	2.47	2.97	7.34
12	Coordinated and organized terrorist attacks	2.55	2.87	7.32
13	Political unrest leading to government collapse and civil disturbance	2.49	2.83	7.05
14	Non-compliance with privacy and data protection laws	2.34	2.94	6.88
15	Random attacks of extreme violence	2.48	2.66	6.59
16	Serious supply chain disruption causing significant financial loss	2.37	2.71	6.42
17	CBRN (chemical, biological, radiological, nuclear) attack on a large city	2.23	2.62	5.84
18	A new cold war between East and West	2.17	2.26	4.90
19	Military conflict between U.S. and North Korea	2.15	2.28	4.90
20	Uncertainty over UK/EU Brexit negotiations	2.02	2.06	4.16

Figure 5: Regional Comparisons against 5 key global risks (percentages)

Risk	Overall %	Americas %	Europe %	Asia %
Technology Failure (Cyber or IT malfunction)	23.54	23.46	27.56	24.67
Supply Chain Failure (all potential causes)	18.87	19.23	18.22	19.33
Political and Economic Instability	17.55	17.28	15.56	18.00
Terrorism and Random Violence	18.84	18.82	18.67	20.00
National Infrastructure Failure	21.19	21.22	20.00	18.00

Figure 6: Sector Comparisons against 5 key global risks (percentages)

Risk	Finance	Energy	Techn	Bus Ser	Health	Other
Technology Failure	23.65	22.22	28.61	23.10	19.95	25.36
Supply Chain Failure	18.24	18.89	17.78	17.62	23.53	16.86
Political and Economic Instability	18.47	20.00	16.94	17.86	17.65	17.65
Terrorism and Random Violence	18.71	23.33	17.22	18.81	20.05	19.22
National Infrastructure Failure	20.94	15.56	19.44	22.62	18.82	20.92

Figure 7: The ranking in terms of how much the issue currently involves resilience professionals

Rank	Issue	Mode value	Median Value
1	Major IT interruption due to technical malfunction or human error	3	3
2	Extreme natural disasters (earthquake, volcano, hurricane, tornado)	3	3
3	Coordinated and organized terrorist attacks	3	3
4	Wide-scale flooding outside of manageable levels	3	3
5	Pandemic which spreads quickly with extensive global fatalities	3	3
6	A man-made disaster to nuclear, chemical, gas, or oil facilities	3	3
7	Random attacks of extreme violence	3	3
8	State-sponsored cyber attacks	3	2
9	Criminal cyber attacks	3	2
10	Severe reputational damage from targeted social media campaign	3	2
11	Serious supply chain disruption causing significant financial loss	1	2
12	Non-compliance with privacy and data protection laws	1	2
13	CBRN (chemical, biological, radiological, nuclear) attack on a large city	1	2
14	Failure of critical national infrastructure in a major country	1	2
15	Political unrest leading to government collapse and civil disturbance	1	2
16	Inadequate investment in information security	1	2
17	A global financial crash as severe as 2007/2008	1	2
18	A new cold war between East and West	1	1
19	Military conflict between U.S. and North Korea	1	1
20	Uncertainty over UK/EU Brexit negotiations	1	1

Geographic and Industry Differences

Because certified professionals had previously expressed interest in learning more about how issues and priorities varied among geographic areas and business sectors, we were able to identify some interesting comparatives on an aggregated risk level from the survey. At this higher level, the issues were addressed were:

- Technology Failure (Cyber or IT malfunction)
- Supply Chain Failure (all potential causes)
- Political and Economic Instability
- Terrorism and Random Violence (domestic and international)
- National Infrastructure Failure (all potential causes)

There was debate about whether climate change or a wider environmental risk category should be included, but from the time-scale of this survey (12 months) it was felt that these longer-term risks would manifest themselves in particular events. Climate issues might create more extreme weather, which could then impact supply chain and/or national infrastructure disruptions.

The results are presented by region (see Figures 5, page 12) and confirm that cyber/technology risks are now the highest concern in all regions. Generally, there seems to be little difference of opinion amongst resilience professionals regardless of region, again demonstrating the global nature of business and the common threats faced by all.

Within the regional rankings only North America, Europe and Asia were itemised as there was insufficient participation from other regions to give a meaningful comparison.

Although all business sectors were invited to participate, the areas with the top response rates were finance, energy, technology, business services, and healthcare. A miscellaneous other category is included to cover all the other sectors that responded (see Figure 6, page 13). Although technology does not score the highest in every sector, it is still an important issue for all sectors. Within the energy sector, terrorism and random violence scored slightly higher than technology. Within the healthcare sector, supply chain failures and terrorism and random violence both score marginally higher than technology.

Professional Involvement

As previously indicated, the ideal response would be 3 (indicating a strong involvement of the resilience professional, but working jointly to achieve solutions with other affected functions). We looked for responses where both MODE and MEDIAN values would be 3 and found 7 of the 20 items achieved this, but these are the traditional incident response and disaster recovery issues that business continuity professionals are expected to address. Three other items scored 3 on mode and 2 on median which is good given that are cyber related and reputational damage issues where other departments might be expected to take the lead. Several items scored poorly on mode (1) but did score better (2) on median. These are not traditional business continuity issues such as supply chain disruption, compliance and financial crisis management. Although much more is needed to be achieved, some increased involvement is a positive development.

Resilience professionals are generally not involved at all on a few issues. This is perhaps to be expected given they are large scale political, economic, or social threats which are beyond the control of individual organizations. However, it is still important that they are involved in contributing to the strategic planning needed to deal with potential consequences of these threats.

In conclusion

This annual report provides valuable insight into many of the issues that face resilience professionals today. It is a unique view because it not only takes input from industry thought leaders but also allows DRI certified professionals the chance to comment on the practicality of such opinion. In particular, the Top 8 Global Trends section of the report shows both the positive progress being made by the profession as well as those aspirations that are proving difficult to achieve.

An important positive is the emergence of a much wider involvement in following the Professional Practices across many countries and across virtually all business sectors. The time when the profession was perceived as mainly about IT and financial services in developed countries seems to be over. The community is much more diverse and much more open to involvement in a wider range of disruptive issues that are potentially damaging to their organization.

However, there seems to be less involvement with strategic risk management, horizon scanning, and even cyber incident response than we had hoped to see. This might indicate a slowing up of the trend to integrate the various risk disciplines into an overarching resilience framework that many industry experts have long predicted. In any case, DRI will be following these issues as well as all those that effect our profession and regularly sharing what we learn with the resilience community.

The once apparent inevitability of risk management, business continuity, and information security merging has not materialized to any significant degree. We are a long way from the acceptance of a common, overarching resilience management discipline.

About 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.

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.

Mary Gardner is the VP business resilience for Zurich in North America (ZNA). At ZNA, Gardner brings broad industry knowledge and a multidimensional approach. She is responsible for establishing an enterprise-wide crisis management and business recovery framework by working with senior management in all business areas and with Zurich's suppliers and sourcing partners. Prior to joining ZNA, Gardner was the director of business risk for major international companies including retail, consumer brands, telecommunications and cable industries. She also spent 12 years with international insurance brokerages. She holds a Bachelor's degree in Business Administration/Management and an Executive MBA from the University of Denver.

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.

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). Richard'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

DRI International is the non-profit that helps organizations prepare for and recover from disasters. This is achieved this through education, accreditation, and thought leadership in business continuity and related fields. Founded in 1988, DRI has more than 15,000 certified individuals in 100+ countries, and 94 percent of all Fortune 100 companies employ DRI certified professionals. In addition to certifying individuals, DRI assesses organizations to determine resilience and offers organizational accreditation.

As a recognized expert resource, DRI acts in an advisory capacity to organizations and government institutions worldwide, helping to develop professional standards and promote greater resilience. DRI is a member of the United Nations Office for Disaster Risk Reduction's (UNISDR) Private Sector Working Group ARISE Initiative and was on the business and industry delegation to the negotiations of the Sendai Framework for Disaster Risk Reduction. DRI is also an ANSI-accredited Standards Development Organization, a CQI and IRCA Approved Training Partner, and an International Organization Liaison Observer to ISO/TC 292 for standardization in the field of security to enhance the safety and resilience of society.

To further its outreach efforts, DRI introduced the 501(c)(3) non-profit Disaster Recovery International (DRI) Foundation. The Foundation's mission is to promote disaster risk reduction through partnership and education, as well as aid recovery efforts through fundraising and volunteerism. The Foundation is also committed to supporting veterans through the Veterans Outreach Program.

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