2025 — Risk And Resilience Trends

11th Annual Report

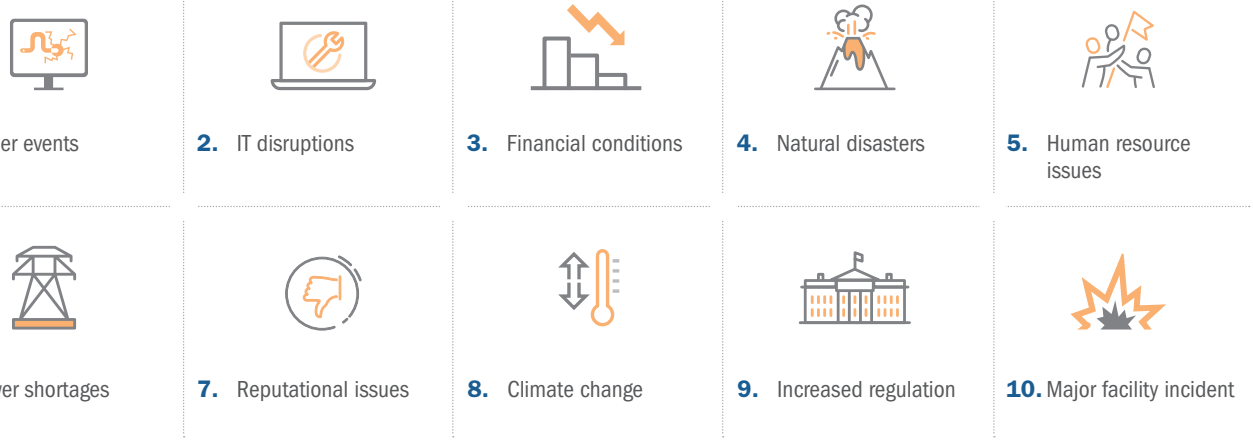
Executive Summary

The DRI International Global Risk and Resilience Trends Report is issued annually and is now in its 11th year. It aims to provide a comprehensive view of risk and resilience trends and comments on how traditional business continuity is being modified to meet these challenges. Prepared in conjunction with the DRI Future Vision Committee (FVC), it delivers a fully independent analysis. The FVC consists of international thought leaders and experts in aspects of business that are associated with resilience. The main findings are drawn from the 2025 DRI International Risk and Resilience Survey. Conclusions are formulated from both this survey, other appropriate sources, and the direct experience of FVC members.

The main contributors to the survey are practitioners in business continuity, organizational resilience, operational resilience, disaster recovery, crisis management, and emergency management. These specializations form the bulk of what is viewed as resilience within organizations. However, care must be taken in adopting a specific definition of a resilience professional. The discipline is evolving, and in its emerging format, there are many different definitions and ongoing debates regarding its precise scope.

The 2025 *Risk Index* (Figure 1, page 2) shows the current top 10 current resilience concerns as reported in the survey.

Figure 1: Top 10 resilience concerns as reported



The survey also focused on selected longer-term strategic risks and revealed the top five risks highlighted by respondents in order of importance (Figure 2, below).

Figure 2: Top five risks highlighted by respondents

1.	Uncontrolled/unregulated use of artificial intelligence (AI)
2.	Lack of trust in organizations and institutions to deal with future challenges
3.	Changing alliances and geopolitical conflicts
4.	Eco-system tipping points
5.	Lack of natural resources to sustain a modern economy

The top 15 risks are all further analyzed from a regional, business sector, business size, and regulatory status perspective. Full *Risk Index* figures are presented for all of these.

As well as discussion on the survey findings, there is an assessment of how practices and priorities have changed over recent years and the direction of travel expected for the discipline. This year, the survey includes additional questions that relate to cybersecurity and how it is managed in organizations, particularly its relationship with other resilience functions.

2025 Overview

The Trends Report is issued annually and monitors internal and external risk trends that impact the ability of organizations to be resilient. A resilient organization is one that proactively challenges disruptive incidences. All organizations are subject to risk, some from external events over which we have little or no control, and others from incidents such as protests and labor strikes for which we can plan. This report showcases how investing in resilience is helping to remove some of the uncertainty faced by our organizations.

It is fair to argue that as the world has become riskier and less predictable, the outcomes faced are more varied and with potentially greater damage. Many will share increasing concern about the instability faced in various aspects of our lives. Politics, economics, social demands, and environmental issues are rapidly changing and can become contentious. Disruptions seem to occur daily with many having significant and immediate impact on organizations' operations.directly impacting resilience. Uncertainty breeds unexpected outcomes which challenge the secure foundation for effective resilience programs. Long established assumptions must be consistently revisited to ensure plans and processes remain relevant.

The concept of horizon scanning is useful for resilience professionals, and this report highlights areas for consideration. While some issues cannot be resolved overnight, certain potentially negative outcomes can be identified, addressed, and built into working practices to ensure better preparedness in the future.

The FVC outlined six key issues that resilience professionals need to monitor:

1. Global politics, economic, and social changes
2. Regional wars and conflicts
3. Disruptions of global supply chains
4. Climate-related risks
5. Artificial intelligence (AI)
6. Energy and water policies

While practitioners may not be able to mitigate all impacts, they will be able to analyze the scale and scope of the risks and fortify their towards them.

Many organizations have taken steps to mitigate the impact of total dependency on supplies from countries or regions affected by internal conflict, trade wars, or severe weather. However, the organization's degree of globalization (including its supplier base) is so embedded in business operations it cannot easily or quickly be modified. Even though some organizations are moving towards onshoring or nearshoring practices to reduce supply chain risk, the risk is difficult to mitigate in the short- or medium-term. An example of this is the 2020-22 semiconductor shortage due to factory closures in Asia from COVID-19. At the time, Taiwan provided 92% of the most advanced logic semiconductors and, despite the shortage, the country continues to be the primary global supplier. Efforts have been made to start up similar manufacturing facilities in the U.S., for example, but emulating Taiwan's manufacturing environment is challenging due to labor rights and cost issues.[1]

The world is dangerously poised in its needs for oil and gas, electricity, water, and precious metals. While some countries attempt self-sufficiency for these commodities, most of the world depends on cooperation and strong global trade. In a world where tariffs dominate, resources are not distributed equitably, and global conflicts are rife. Resilience professionals cannot ignore the potential impacts to their organizations, and resilience should now be the strategic backbone of any organization.

Reduced social unity is also a social trend that is being observed across large parts of the world. Polarizing views, fake news, conspiracy theories, along with the anonymity and speed at which news can be published on social media are contributing to lack of empathy and even hatred. The use of intense disinformation and misinformation campaigns to destabilize national politics is now well-documented and beyond doubt.[2]

Another area affected by global trends is the increasing evidence of cyber-attacks on national resources by hostile states, with government-sponsored cybercrime already a reality. The recent attack on Jaguar Land Rover in the UK is suspected to be a result of state-sponsored cybercrime[3], and the U.S. House Committee on Homeland Security reintroduced legislation earlier this year to combat growing threats from the Chinese government against the nation's critical infrastructure[4] are just two examples. Such legislation is also helpful for resilience practitioners as it highlights the potential devastation of state-sponsored attacks to senior management.

A more recent risk concern is the weaponization of AI. While AI has the potential to provide huge benefits to organizations, it comes with risk. Today, the validity of the tool varies with application. AI is still relatively new and relies on large, reliable datasets to generate accurate and repeatable results. Risks emerge when AI results are presented as fact, without testing or validating. Furthermore, the malicious use of AI – such as the use of deepfakes to emulate executives, for example – is starting to cause significant disruption and financial loss for organizations.[5] AI is, at its core, a broad field of computer science which requires data security, connectivity, and power demands. Some studies have suggested that the energy demands of AI and related data centers may be less than currently estimated but will still be significant.[6]

Electricity security is already fragile in many parts of the developed world, and the possibility of electricity rationing and unplanned blackouts, as already seen in South Africa[7], is a very real threat. After many years of unpopular public sentiment, nuclear power is back on the political agenda. However, there is no disagreement that in the future there will be an increased need for diversification of energy types.

Part 1 — 2025 Survey Results

The Future Vision Committee (FVC) defined a set of 15 barriers to resilience which were included in this year's survey (Figure 3, page 5). The FVC also identified five longer-term global and strategic risks and asked a separate question for respondents to consider. Responses were received from a variety of job titles across all business types, sectors, sizes, and geographies and were categorized into four international regions.[8]

It is important to note that AI appears in two sections of the report. In the Key Risks section, AI refers to the current risks and concerns within the respondents' organizations. The Strategic Risks section addresses AI evolution and escalation over the next five years across business as a whole.

Figure 3: The 15 key risks identified by the FVC for this year's survey

#	Icon	Risk (in order of criticality/ highest perceived risk)	Description
1		Cyber events	All disruptive cyber events including ransomware, service denial, information corruption, and data theft.
2		IT disruptions	IT failure resulting in a system or application outage for an unacceptable duration.
3		Financial conditions	Overall state of the domestic and global economy based on a wide range of financial indicators.
4		Natural disasters	Hurricanes, tornadoes, cyclones, seismic events, wildfires.
5		HR issues	Acquiring and retaining staff with current and future skills. The implications of AI on management and professional jobs.
6		Power shortages	Inadequate power to maintain normal operational functionality caused by failure of company or service provider infrastructure.
7		Reputational issues	Propagation of misinformation, memes, and fake profiles to damage company reputation.
8		Major facility incident	Fires, floods, explosions, chemical pollution, construction failures, sabotage, etc.
9		Supply chain disruptions	Disruption of key supplies, supplier failure, low inventories, sole source supplier failure, creating global shortage of commodities and raw materials.
10		AI issues	The implications of current AI technologies on existing jobs including management and professional roles.
11		Increased regulation	Compliance failure leading to financial penalties and possible withdrawal of operating licenses.
12		Climate change	Increased flood risk in coastal areas and drought in hot areas. Impact on future expansion, new construction methods and building protocols.
13		Infectious diseases	Pandemics, epidemics, respiratory illnesses, Ebola-type diseases, and bacterial diseases immune to antibiotics.
14		Terrorism	Domestic and global terrorism, chemical, biological, radiological, and nuclear (CBRN) attacks on high density locations such as transportation hubs or shopping malls.
15		Civil unrest	Activist protestors disrupting roads, transportation systems, and places of work. Injury, damage to buildings, and public disorder.

Probability, Impact, and the Risk Index

A scale of 1 to 5 was used in the survey, with 1 being the lowest and 5 the highest score. For both *probability* and *impact*, a weighted average score across all responses was calculated. To develop a Risk Index, the probability and impact scores were multiplied. This is the same methodology that has been used in every annual survey to date. The rankings are also shown with an overall number calculated by multiplying the probability and the impact score for each risk (Figure 4, page 7).

This pattern is reasonably consistent on a year-by-year basis, although not necessarily backed up by cost analysis. For example, IT disruptions caused by cyber-attacks may cause a lesser impact and lower direct/indirect costs than those caused by internal system failures, for example. However, the high-profile and unpredictable nature of some cyber-attacks cause more reputational damage and management fear than any other type of incident.[9]

The top five risks remain the same as for the previous year. The only minor change is that **Natural disasters** and **Financial conditions** have switched third and fourth position. **Cyber events, IT disruptions**, and **HR issues** have retained the same position over the past three years. Operational risks, such as **Power shortages, Supply chain disruptions**, and **Major facility incident** are mid-table this year. High profile risks, such as those posed by **AI** and **Climate change**, tend to score only moderately in the survey.

As expected, **Infectious diseases** remains low in the list of concerns despite new COVID-19 strains and other diseases on the World Health Organization's (WHO) radar, which could potentially become epidemics or pandemics. The continued drop in the ranking after its 2020-2022 domination may indicate an overconfidence after successfully surviving COVID-19. It is also essential that public health systems are adequately funded and prepared to deal with any future outbreaks of either COVID-19, or a new pandemic or epidemic.

Terrorism and **Civil** unrest continue to be at the bottom of the list, despite the fact that most commentators suggest we face one of the most unstable global political and military landscapes since World War II[10]. While there have been conflicts, wars, and other tensions since World War II, 2024 recorded the highest number of active conflicts since 1946[11].

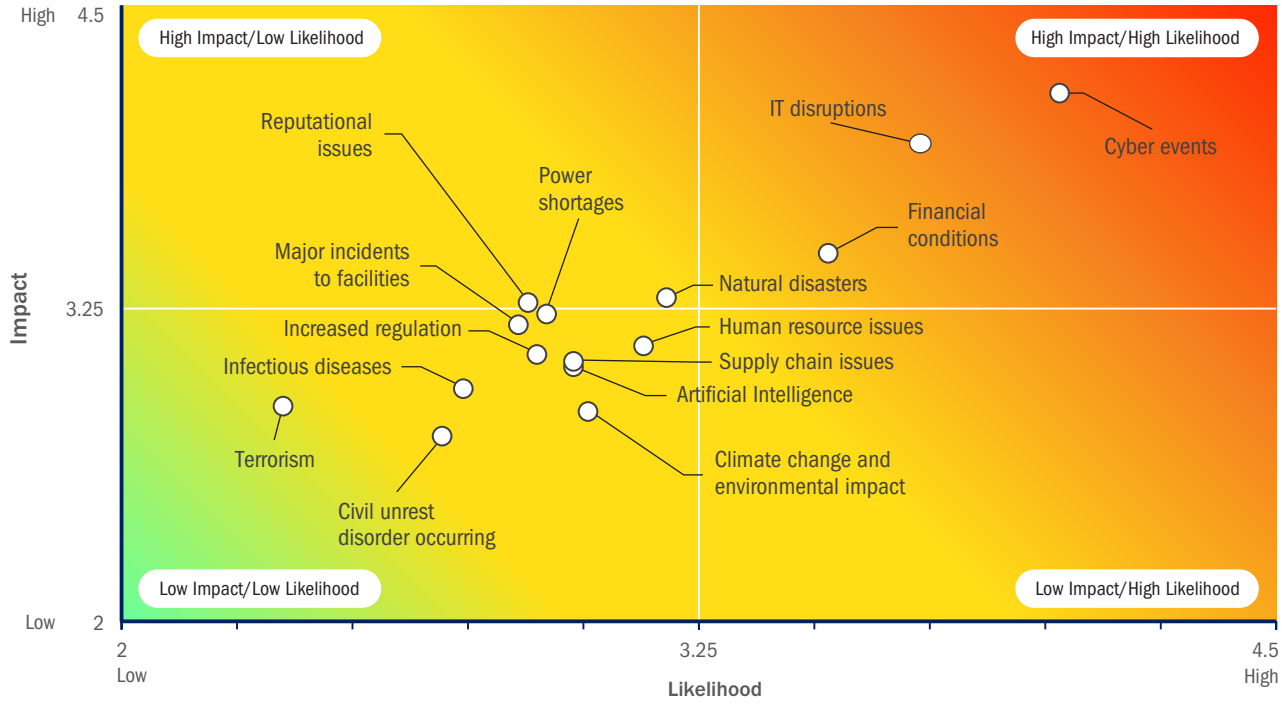
While there are some interesting patterns, the risks generally tend to be high, medium, or low with a few moving significantly among these wider categories. The COVID-19 period did see wide fluctuations, but clearly that was due to an obvious cause. Since then, risks have tended to return to their typical ranges. Climate change was ranked higher in 2024 than before, but it has failed to maintain its position this year. With El Niño helping make 2024 the hottest year on record[12] as well as the sheer volume of climate-related disasters in the same year,[13] the slightly cooler conditions of 2025 are likely to lead professionals to view other risks as greater.

Since 2023, the high-risk items are cyber events, IT disruptions, financial conditions, HR issues, and natural disasters. The medium-risk items are power shortages, reputational issues, major facilities incidents, supply chain disruptions, and AI issues. The relatively low risks are increased regulation, climate change, infectious diseases, terrorism and civil unrest. This is interestingly consistent across different surveys (such as the *Allianz Risk Barometer*[14]) and different years. Terrorism and civil unrest seem to fit into the "unlikely to happen" category and consistently score lower down on the scale of risks. However, is this a warning in itself? Such incidences might be unlikely to happen, but are practitioners prepared if they do? Consistently training staff and exercising even the least likely scenarios are of the utmost importance to ensure the potentially devastating effects of these high-impact events can be mitigated as much as possible.

Figure 4: PROB (probability), IMP (impact), and the combined Risk Index (RI) from the survey

Rank 2025	Icon	Risk	PROB	IMP	RI
1		Cyber events	4.03	4.15	16.72
2		IT disruption	3.73	3.95	14.73
3		Financial conditions	3.53	3.51	12.39
4		Natural disasters	3.19	3.32	10.50
5		HR issues	3.13	3.13	9.79
6		Power shortages	2.92	3.26	9.51
7		Reputational issues	2.88	3.30	9.50
8		Major facility incident	2.86	3.21	9.18
9		Supply chain disruptions	2.98	3.06	9.11
10		AI issues	2.98	3.05	9.09
11		Increased regulation	2.90	3.09	8.96
12		Climate change	3.01	2.86	8.61
13		Infectious diseases	2.74	2.95	8.08
14		Terrorism	2.35	2.88	6.77
15		Civil unrest	2.35	2.76	6.49

Figure 5: Risk Index mapped on a risk matrix



Key Strategic Risks

For reference, the five key strategic risks for resilience professionals identified by the FVC in 2025 (Figure 7, page 9) were also ranked by the survey respondents as to their current resilience priority. The priorities given to each was the same as for the five-year horizon.

The two main strategic risks are the future management of technologies based upon AI and the lack of trust in organizations and institutions to provide sufficient jobs and sustainable career opportunities in the future. The position of the top two strategic risks are consistent with previous years and are likely to remain that way in the medium-term.

From the AI perspective, the well-documented concerns about increased unemployment, the elimination of certain professions entirely, and the change in our perception of developing a career are often discussed, but are other risks that are not so often discussed:

- The possible loss of institutional knowledge when humans are replaced by AI.
- The risk of AI investment taking resources from other areas, including resilience.
- The danger that AI will reduce development opportunities for entry level people when early-stage jobs disappear.

Early-stage jobs already seem to be shrinking, according to the U.S. Bureau of Labor Statistics (July 2025). They report that labor market softening is hitting recent college graduates hard. Data from the "Current Population Survey" shows a troubling pattern for young workers who have recently graduated. Young college graduates between ages

Figure 6: Relative positions over the year since COVID-19 was at its peak concern

Icon	Risk	Position 2021	Position 2022	Position 2023	Position 2024	Position 2025
	Cyber events	2	1	1	1	1
	IT disruption	3	2	2	2	2
	Financial conditions	9	3	4	4	3
	Natural disasters	4	6	3	3	4
	HR issues	5	4	5	5	5
	Power shortages	14	10	7	7	6
	Reputational issues	8	12	6	10	7
	Major facility incident	7	9	9	6	8
	Supply chain disruptions	6	7	11	11	9
	AI issues	X	X	10	12	10
	Increased regulation	13	8	12	9	11
	Climate change	12	11	13	8	12
	Infectious diseases	1	5	8	13	13
	Terrorism	10	14	14	15	14
	Civil unrest	11	13	15	14	15

X = This item was not included in the survey for 2021 and 2022

23 and 27 are experiencing unemployment rates that average 4.59% in 2025 – a stark contrast to the 3.25% rate this same demographic experienced in 2019. Crucially, it is the white collar professions which are being affected the most by "technological disruption", defined in the report as AI and the use of large language models. The IT sector, for example, has traditionally very low levels of unemployment. However, from 2019-2025 unemployment rose from 1.98% to 3.02%. Arts, design, media, and sport has also seen unemployment levels rise by 1.77 percentage points over the same period.[17]

From a lack of trust perspective there was also concern about issues such as ESG and DEI and what decisions are being taken at board level. ESG has the most direct business impact in that it often involves investment strategies,[18,19] especially as it pertains to fossil fuel exploration funding. DEI remains primarily a political issue but does have knock-on effects for organizations – particularly in respect of corporate reputation and PR.[20]

The third strategic risk was changing alliances and geo-political conflicts. This reflects worries about global stability as shifting alliances and ongoing or emerging conflicts persist. Apart from the obvious physical consequences of war, there is also the risk from government-sponsored cyber warfare[21] and the use of commercial means to damage adversary powers.

Finally, the two lowest-rated strategic risks are a general concern about ecosystem tipping points being triggered and the availability of sufficient natural resources for future developments.

For this type of strategic analysis, it is important that professionals take a sophisticated approach to risk scanning. It is inadequate to simply have experience of a risk or a good understanding of it, not least because it can lead to familiarity bias (i.e. prioritizing familiar and known risks over those that are unfamiliar or considered less of a risk). Although many companies already undertake horizon scanning in one form or another, it is vital

Figure 7: Five key strategic risks for resilience professionals identified by the FVC in 2025

#	Strategic risk	Description
1	Uncontrolled/unregulated use of artificial intelligence (AI) and other new technologies	We are currently seeing a range of technologies based on AI that have potential for improving productivity and efficiency. They will inevitably lead to a major reconstruction of the labor market with unpredictable social consequences. They can – and already are – being used for unethical purposes – compromising the safety, security, and privacy of individuals, companies, regions, and countries. Other emerging technologies, such as quantum computing, can pose serious security risks when used maliciously.
2	Lack of trust in organizations and institutions	Limited confidence in ability of governments, financial institutions, and corporate boards to properly address complex social problems. Inadequate consideration of ESG as organizations shy away from investment, and the impact of DEI rollbacks on organizational reputation .
3	Changing alliances and geo-political conflicts	Geo-political changes resulting from armed conflict, state terrorism, and fomenting political protest in other countries. New alliances formed from security, economic, and commercial imperatives. Factors include the strategic use of foreign aid, imposition of sanctions, and governmental retaliation against nations that it sees as hostile.
4	Eco-system tipping points	The proximity of irrevocable changes to eco-systems that can affect food supplies, the habitability of coastal region and island nations, and biodiversity. Secondary and tertiary impacts will adversely impact supply chain disruption, increased natural disasters, public health, and civil unrest.
5	Lack of natural resources to sustain a modern economy	As countries pivot away from fossil fuels towards renewables and nuclear and a growing population drives energy demand higher, there could be intermittent power supply shortages in the medium term. Water is also an increasingly scarce resource and difficulties of desalination at scale are significant.

to consider the wider spectrum of risks rather than those already experienced or considered likely to experience. Consulting national risk reports, risk barometers, or attending forums with other risk and resilience professionals are tried and tested ways for professionals to become better acquainted with the wider risk environment. It is also important to understand that horizon scanning is not about predicting the future. It is about identifying potential unexpected or rare risks, understanding the possible consequences of those risks, and ensuring that adequate response strategies are identified. Some risk specialists argue that the process also can identify unexpected opportunities which can be exploited by business.

Regional Overview

The survey looked at four continental regions plus a consolidated others category.

North America: U.S. and Canada

Latin America: South America and Mexico

Europe: EU and non-EU countries in Europe

Asia: Japan, South-East Asia, the Indian subcontinent and the Middle East

Others: Africa, Australia and New Zealand and some small island nations

At a country level the top 4 countries were the United States (58.0%), Canada (12.6%), United Kingdom (5.0%), and India (3.4%). A total of 36 countries provided input to the survey.

Figure 8: Risk Index rank for individual regions

Rank	Icon	North America (NA)	Icon	Latin America (LA)	Icon	Europe (EU)	Icon	Asia (AS)
1		Cyber events		Natural disasters		Cyber events		Cyber events
2		IT disruptions		IT disruptions		IT disruptions		IT disruptions
3		Financial conditions		Cyber events		Financial conditions		Natural disasters
4		Natural disasters		Increased regulation		HR issues		Power shortages
5		HR issues		Climate change		Reputational issues		Reputational issues
6		Reputational issues		Power shortages		Increased regulation		Major facility incident
7		Power shortages		Reputational issues		Power shortages		Financial conditions
8		Supply chain disruptions		Major facility incident		AI issues		HR issues
9		Major facility incident		HR issues		Supply chain disruptions		Climate change
10		Climate change		AI issues		Major facility incident		Infectious diseases
11		AI issues		Infectious diseases		Climate change		Terrorism
12		Increased regulation		Civil unrest		Infectious diseases		AI issues
13		Infectious diseases		Financial conditions		Natural disasters		Civil unrest
14		Civil unrest		Supply chain disruptions		Civil unrest		Increased regulation
15		Terrorism		Terrorism		Terrorism		Supply Chain Disruptions

Regional Variations

While the top two risks, cyber and IT disruptions (not caused by cyber threats), lead the overall lists there is a slight variation in Latin America where natural disasters are the top concern. Conversely, natural disasters are only ranked 13 in Europe against the survey average of four. Obviously, natural disasters are very location specific and northern Europe – where the bulk of the European responses came from – is less prone to them than other regions.

Other results that appear to be unexpected or very wide of the average include financial conditions being ranked 13 in Latin America against a survey average of three. This is difficult to reconcile with the known economic situation. For example, with U.S. tariffs of 50% on Brazil and ongoing financial weakness in Argentina – the two largest economies in South America – it is likely to be skewed by the sample of individuals answering the survey from the region: 50% are from banking, 13% from business services, 13% from government, and 12% from non-profit organizations. Only 13% were from general commercial activities and most of that group was from technology.

Supply chain disruptions are ranked 15 in Asia whereas the survey average is nine. China, South Korea, and Taiwan, plus and other countries in South-East Asia manufacture the majority of goods sold in North America and Europe. The current political environment surrounding imports and exports between certain nations has the potential to create significant disruption in supply chains. However, dislocation of

Figure 9: Risk Index regional comparisons

Rank	Icon	Risk	NA Rank	LA Rank	EU Rank	AS Rank
1		Cyber events	1	3	1	1
2		IT disruption	2	2	2	2
3		Financial conditions	3	13	3	7
4		Natural disasters	4	1	13	3
5		HR issues	5	9	4	8
6		Power shortages	7	6	7	4
7		Reputational issues	6	7	5	5
8		Major facility incident	9	8	10	6
9		Supply chain disruptions	8	4	9	15
10		AI issues	11	10	8	12
11		Increased regulation	12	11	6	14
12		Climate change	10	5	11	9
13		Infectious diseases	13	6	12	10
14		Terrorism	15	15	15	11
15		Civil unrest	14	12	14	13

supply chains would also have serious consequences for Asian nations, which is perhaps not fully demonstrated here. The majority of survey participants sample from Asia are from the banking and financial services sectors (nearly 60%). They rank supply chain disruptions as their third from bottom risk.

In North America and Europe, many firms have attempted to diversify their sources of supply. However, this is a difficult task given that some suppliers will be on long-term contractual arrangements with no break clause. Additionally, raw materials might only be available in limited countries with very few suppliers – or even just a single supplier. Setting up a domestic manufacturing or assembly plant is often a costly and relatively slow process.

There is also a political dimension when one country uses its virtual monopoly position over a vital raw material to exert pressure on another country and its allies. The most serious current case is rare earth minerals and China's control of their refinement. It has huge impact on U.S. industry and defense capabilities and is an issue at the highest levels of government.

Infectious diseases appear at number six for Latin America against a survey average of 13. This is the only region where this number has not fallen steeply since the end of COVID-19. This is probably because of the publicity this year about the Oropouche virus outbreak[22] as well as other scares such as chagas disease and dengue fever.[23]

Sector Overview

The survey looked at the business sectors represented by the respondents.

Given the wide range of possible answers, the results were grouped into larger sectors for trend analysis purposes. It is accepted that within these consolidated categories there might be some additional variability, but these variations are relatively small.

The six consolidated sectors listed here contributed 91.2% of the answers received.

- Finance (including banking, brokerage, and insurance) — 27.2%
- Industrials (including manufacturing, transportation, and retail) — 21.9%
- Public Sector, Charities, and Non-profit — 12.3%
- Healthcare (including hospitals) — 11.9%
- Technology (including IT and telecoms) — 10.2%
- Business Services (including consultancy, audit, and recruitment) — 7.7%

Sector Variations

There is a much wider variance between sectors than between regions. This is to be expected because some risks are directly related to the type of work undertaken in a particular sector. However, some fundamental business functions or services – such as technology, finance, HR, and utilities – are common to all business entities. Other risks are greater in some sectors than others, although these results are consistent with previous surveys.

Examples of risks rated significantly higher than average include supply chain (industrials), reputation (finance and business services), infectious diseases (health), AI (technology and finance), and major facilities incident (government and healthcare).

Examples of risks rated with significantly lower than average importance include AI (industrials, healthcare, and public sector), climate change (business services and technology), financial conditions (public sector), and HR issues (public sector).

The most apparent difference is between government and public sector responses. Serious commercial concerns such as finance, HR, and supply chains score much lower in the public sector – whereas public order issues like terrorism and civil unrest score much higher. These overall trends are not unreasonable given the nature of the work in different sectors.

Figure 10: Risk Index ranking for each of the six grouped sectors

Survey Rank	Icon	Finance	Icon	Industrials	Icon	Public Sector & Non-Profit
1		Cyber events		Cyber events		Cyber events
2		IT disruptions		Financial conditions		IT disruptions
3		Financial conditions		IT disruptions		Natural disasters
4		Reputational issues		Supply chain disruptions		Major facility incident
5		AI issues		Reputational issues		Power shortages
6		Increased regulation		Increased regulation		Terrorism
7		Natural disasters		Natural disasters		Infectious diseases
8		Power shortages		HR issues		Civil unrest
9		HR issues		Power shortages		Reputational issues
10		Major facility incident		Major facility incident		Climate change
11		Climate change		Terrorism		Financial conditions
12		Infectious diseases		Climate change		HR issues
13		Supply chain disruptions		AI issues		Supply chain disruptions
14		Terrorism		Civil Unrest		AI issues
15		Civil unrest		Infectious diseases		Increased regulation

Survey Rank	Icon	Healthcare	Icon	Technology & Telecoms	Icon	Business Services
1		Cyber events		Cyber events		Cyber events
2		IT disruptions		IT disruptions		Reputational issues
3		Financial conditions		Financial conditions		IT disruptions
4		Major facility incident		AI issues		Financial conditions
5		Infectious diseases		Natural disasters		HR issues
6		Natural disasters		Reputational issues		AI issues
7		HR issues		Power shortages		Power shortages
8		Supply chain disruptions		HR issues		Natural disasters
9		Power shortages		Major facility incident		Increased regulation
10		Increased regulation		Increased regulation		Major facility incident
11		Reputational issues		Civil unrest		Supply chain disruptions
12		Terrorism		Supply Chain Disruptions		Civil Unrest
13		Climate change		Terrorism		Infectious diseases
14		AI issues		Climate change		Terrorism
15		Civil unrest		Infectious diseases		Climate change

Traditionally, the industrial sector has been somewhat of an outlier with physical interruptions higher than elsewhere and of less concern over business and organization issues. However, this year, apart from the expected above average ranking for supply chain disruptions and the lower-than-expected score for AI risks, there is no other significant difference.

Organization Size and Type

Respondents assigned their organization to one of six categories. The percentage of each category is:

- Multinational Corporate — 27.6
- Large Domestic Business — 20.7
- Small or Medium-sized Business — 14.5
- Niche Business (below 50 staff) — 8.4
- Government Related — 16.5
- Non-profit/Charities/Universities — 10.8
- Other (not specified) — 1.5

Size and Type Variations

Increased regulation is an important issue for all commercial organizations – in particular multi-nationals (who must comply with global, national, and regional regulations) and small companies (who have limited resources to deal with additional enforced overheads). Increased regulation is of lesser concern in the government and non-profit sectors. This is, perhaps, surprising as non-profits are subject to much financial scrutiny while governments enforce laws and regulations.

Reputation is an increasing concern to all commercial sectors, particularly multi-nationals, small- to mid-sized enterprises (SMEs), and niche organizations. It is also of concern in the government and non-profit sectors, but at a lower level than in the commercial sectors. In the age of instant media, adverse publicity can damage a brand resulting in reduced market valuation, immediate loss of revenue, and loss of market share. A dramatic example of this came in 2023 when a leading beer brand, Bud Light, badly misjudged its primary market. It switched its advertising to attract a younger clientele but instead alienated its traditional customer base. The strategy failed and the brand saw an 11% decline in sales in the month of the controversy. Sales remain well below the traditional levels and it has lost its market leadership status.[24] Even after two years it is still struggling to restore its credibility. Although this is a strategic marketing error, any mismanaged issue that causes an organization to lose public or client support has serious consequences.

AI risk is a risk for multinationals, SMEs, and niche companies but a lower concern elsewhere. However, AI is clearly a wider issue than just the risks it might create – it is an opportunity for an organization to improve its efficiency, performance, and quality. Although it may present a challenge to some resilience practitioners, overall, it could be an opportunity to make an organization more resilient and less prone to error.

Infectious diseases is perceived as high risk in government and non-profit organizations. However, it has become a relatively minor risk for others, with multinationals and SMEs seeing it as their lowest concern. This is a worrying trend and shows a view that because COVID-19 was survivable, the lessons learned could be transferred to another pandemic or epidemic situation and nothing further needs to be done. There needs to be a constant state of readiness against such an eventuality – it is very unlikely that COVID-19 will be the last pandemic we have to face, and the next pandemic is unlikely to require a different response to that required for COVID-19.

Civil unrest is a low-level threat in most sectors but with slightly more relevance to the government sector. This is an area that more attention should be paid to as social and political unrest continues to trouble most western nations.

Terrorism is a low-level threat in all commercial sectors but is of much higher concern in both government and non-profit sectors. This is another issue that deserves more attention in commercial business – it is a rare occurrence but a devasting one if it does happen.

Figure 11: The risk ranking for each of the seven reported grouped sectors

Rank	Icon	Multinational Corporates	Icon	Large Domestic	Icon	Small Or Medium (SMBs)
1		Cyber events		Cyber events		Cyber events
2		IT disruptions		IT disruptions		IT disruptions
3		Financial conditions		Natural disasters		Financial conditions
4		Reputational issues		Financial conditions		AI issues
5		Increased regulation		Major facility incident		Reputational issues
6		AI issues		Power shortages		Increased regulation
7		Power shortages		Supply chain disruptions		HR issues
8		Natural disasters		Reputational issues		Major facility incident
9		HR issues		Increased regulation		Natural disasters
10		Major facility incident		HR issues		Power shortages
11		Supply chain disruptions		Infectious diseases		Supply chain disruptions
12		Terrorism		Climate change		Climate change
13		Climate change		Ai issues		Terrorism
14		Civil unrest		Terrorism		Civil unrest
15		Infectious diseases		Civil unrest		Infectious diseases

Rank	Icon	Niche Business	Icon	Government Related	Icon	Non-profit, Charities & Universities
1		Cyber events		Cyber events		Cyber events
2		IT disruptions		IT disruptions		IT disruptions
3		Reputational issues		Natural disasters		Infectious diseases
4		Power shortages		Major facility incident		Natural disasters
5		Financial conditions		Power shortages		Financial conditions
6		HR issues		Terrorism		HR issues
7		Increased regulation		Infectious diseases		Major facility incident
8		AI issues		Reputational issues		Power shortages
9		Infectious disasters		HR issues		Terrorism
10		Natural disasters		Supply chain disruptions		Increased regulation
11		Supply chain disruptions		Civil unrest		Reputational issues
12		Civil unrest		Financial conditions		Supply chain disruptions
13		Major facility incident		AI issues		Climate change
14		Terrorism		Climate change		Civil unrest
15		Climate change		Increased regulation		AI issues

Impact of Regulation on Resilience

Regulated organizations were those in banking, energy, pharmaceuticals, aerospace, and utilities. These sectors have industry specific regulation. Naturally, all firms must also comply with national and corporate law in their individual countries. Some multinational firms may operate and be required to comply with rules in multiple jurisdictions where regulation is very different to that in their home country. The best example is probably financial services regulation on operational resilience (such as the Digital Operational Resilience Act – DORA – in the European Union), where some firms apply tight regulations to all of their global entities to ensure they can future-proof upcoming changes.

Across the entire survey, 80.5% of respondents came from regulated firms and 19.5% from non-regulated firms.

The differences between both are negligible. The only real difference is the expected importance paid to the risk of increased regulation by regulated firms (position eight) as opposed to non-regulated firms (position 13), as shown in Figure 12 below.

Figure 12: The Risk Index ranking for regulated and non-regulated firms

Survey Risk Rank	Icon	Regulated Firms – Rank	Icon	Non-regulated Firms - Rank
1		Cyber events		Cyber events
2		IT disruptions		IT disruptions
3		Financial conditions		Financial conditions
4		Natural disasters		Reputational issues
5		Reputational issues		Power shortages
6		Major facility incident		HR issues
7		Power shortages		Natural disasters
8		Increased regulation		Major facility incident
9		HR issues		Supply chain disruptions
10		Supply chain disruptions		Infectious diseases
11		AI issues		AI issues
12		Infectious diseases		Terrorism
13		Terrorism		Increased regulation
14		Climate change		Civil unrest
15		Civil unrest		Climate change

Part 2 – Resilience Practice

Overview

Over several years, many professionals have seen their job titles change from business continuity manager to resilience manager. The resilience title might be prefixed with operational, organizational, enterprise, or business. However, this is far from universal. There are clearly defined differences between business continuity and operational resilience in some sectors and regions. For example, financial services firms usually have separate business continuity and operational resilience departments. Roles in this sector fall under national operational resilience regulation. In some countries (e.g. the Middle East and South America) business continuity is now mandated and therefore "resilience" titled roles are fewer.

However, regardless of regulatory needs, business continuity still has a defined place in most organizations. There are accepted professional practices specifically for business continuity and, although there are national and international standards for resilience, they have not as yet established agreed professional practices to support them. Until there is more industry agreement, it is difficult to claim resilience is a fully defined practice, unlike business continuity.

In many organizations, business continuity was traditionally treated as a specialist function rather than a core part of the business. Organizations had difficulty in agreeing where it should report. However, it is now generally understood to be an important part of the overall risk management process. Many firms have a Chief Risk Officer (CRO) who operates at the upper levels in the organization with strategic objectives. Resilience and business continuity now often fall under the remit of the CRO.

We are also seeing a small increase in the number of Chief Resilience Officers, although they would typically be below board level of the organization and report into the board (typically to the CRO). However, it is more common that the person with ultimate responsibility at C-Suite level will be another C-level executive. For example, in the UK, the Chief Operations Officer is responsible for operational resilience and will be held personally responsible if the company falls foul of regulations.

The next part of the survey reviews how respondents' organizations currently manage resilience, and how respondents would *like* resilience to be managed.

Figure 13: Resilience Management Approach

Approach	Current Situation	Desired Situation
No one is responsible for resilience across the organization.	8.8%	6.9%
Resilience responsibilities are very fragmented across departments.	29.9%	6.5%
We have an integrated approach to dealing with resilience with several functions reporting to a senior manager.	37.6%	46.4%
We have a CRO who is responsible to the board for all business resilience policies and practices.	23.8%	40.2%

Practitioners perceive their organizations to be lagging in their management of resilience compared to where they think they should be. At the most advanced end of the range – with integrated management and reporting to either a senior manager or a CRO – 61.4% are operating in that manner compared to a desired situation of 86.6%; a gap of 25.2%.

This compares with a gap on the same basis in 2024 of 21.1% – so it appears the situation has not improved. It is expected that more focus on operational risks and better awareness of the consequences of failure should improve companies' awareness of the importance of a more holistic approach. It has been long-argued that the most resilient organizations have strategies that cut across all parts and levels of an organization, often with a bottom-up approach. However, the silo mentality and fragmentation of responsibilities often remain. A more integrated cross functional approach should improve understanding and communications between individuals and across departments.

Cybersecurity is the Most Important Risk to Resilience

The greatest risk to resilience over the past decade has been cybersecurity, according to respondent answers. Even during the COVID-19 period when infectious diseases was the highest ranked risk, cyber always came a close second. This raises concerns about how cybersecurity and business continuity/resilience interact within organizations to create a cyber resilience strategy.

The survey considered the extent to which respondent organizations had been hit by a cyber-attack:

FIGURE 14: Respondent organizations hit by a cyber-attack

Routine attacks detected by information security without serious business impact	68.3%
Compromised systems/data that required system shut down	18.8%
No attacks known	17.3%
Some reputation damage but limited financial loss	12.4%
Ransomware attack that caused system outages	12.1%
Theft of personal data that required external disclosure	11.7%
Theft or corruption of internal data with no direct customer impact	10.6%
Major reputational damage with widespread media coverage	5.3%
Compromised regulatory compliance	4.2%
Significant trading and/or financial losses	3.8%
Significant impact on share price	1.9%

Given that many routine issues would not be reported and the respondents to this survey might not be privy to information regarding cyber-attacks in their organization, it is likely that these figures are lower than the true picture. However, they do demonstrate the scope and scale of the security challenges being faced every day in organizations.

How Does Management View the Importance of Cybersecurity?

Figure 15: Management's view of cybersecurity

LEVEL 1 - failure to manage a cyber breach is the biggest single risk to the survival of the business	39.6%
LEVEL 2 - the business impact of a breach could be a very widespread and costly issue	37.7%
LEVEL 3 – there is a need to have business continuity program in place for when security is breached	7.5%
LEVEL 4 - main focus is on prevention with view that not all attacks can be prevented	6.8%
LEVEL 5 – the full implications of failure are not well understood	3.0%
LEVEL 7 – It is somewhat important - but only one of many risk issues of equal concern	3.4%
Not at all important or no answer	1.9%

There is no doubt that most organizations understand the cyber risks they face and the need to address them effectively. The potential impact a cyber-attack has on an organization from a reputation, cost, and regulatory perspective is understood at all management levels. For example, M&S, a UK retail giant, had their online business suspended for 46 days as a result of a cyber-attack with massive impacts on their overall sales, financial performance, market valuation, and corporate image. The estimated loss has been set at around £300m – a huge loss even for a company of its magnitude. It also had other major impacts such as departure of their Chief Digital Officer only months after the attack.

What Type of Cyber Breach Would Have the Most Business Impact?

Respondents were asked to rate the importance of nine effects a cyber-attack based on their own organization with 1 being most important and 9 being least important.

Based on a weighted average, the consequences were in the following order:

1. A successful ransomware attack
2. An attack causing immediate system and service shutdown for at least several hours
3. Theft of customer and supplier data
4. Theft of confidential and crucial business intellectual property (IP)
5. An attack with embedded malware causing delayed system failure when triggered
6. Data corruption over an extended period
7. Theft of employee private records
8. Theft of confidential financial records
9. A successful attack on process control systems

The item appearing at the bottom of the list (a successful attack on process control systems) is likely to have such an aggregated low score because of the higher levels of response from finance and business service organizations. Respondents from the industrial sectors (manufacturing, distribution, retail, and energy) ranked it as joint second, only behind "an attack causing immediate system and service shutdown for at least several hours." Of course, an attack on process control systems is likely to have a similar effect anyway.

At a national administration level, it is likely to be a significant issue. State sponsored cyber-attacks on process control systems for critical national infrastructure has the potential to cripple businesses. Protection against cyber-attacks on nuclear facilities, electricity generation plants, oil and gas distribution networks, and digital networks should be seen as a top priority for national governments.

How Well Does Business Continuity or Resilience Work With Cybersecurity?

From the results of the survey, it appears that cybersecurity works closely with both business continuity and the wider risk management community.

Despite the closeness of the cooperation at a practical level, there are still many organizations where there is not an overarching top-level executive responsible for both functions. This might create issues with work prioritization or disagreements about overall policy direction, but there is no evidence in the study to indicate that such a problem exists. However, business continuity, cybersecurity, and IT do need to work closely together to combine the technical expertise of IT and cyber professionals as well as the business continuity/resilience expertise of business continuity. Another concern is that only 75% of organizations have risk management and cyber teams working closely together. Cyber teams typically do not fully appreciate resilience, and resilience professionals are usually not technical specialists, making communication a challenge.

Figure 16: How cybersecurity, risk management, and business continuity work together

	Yes	No	Don't Know
Do cybersecurity and business continuity work closely together?	77.0%	19.2%	3.8%
Do cybersecurity and risk management work closely together?	78.0%	16.9%	5.1%
Do business continuity plans cover business interruptions due to cyber events?	80.8%	15.9%	3.3%
Do business continuity tests and exercises use scenarios based on cyber events?	73.2%	20.4%	6.4%
Do information security and business continuity report to the same C-suite executive?	54.7%	40.0%	5.3%

The Implications for Business Continuity

As we see many organizations shifting towards a more holistic approach to resilience, business continuity is clearly in the driving seat for this change.

Now, business continuity benefits from its acceptance as a well-defined profession. In some countries, the International Standards Organization ISO 22301 offers a proven route to formal company certification. Although it is a standard and not a guarantee of compliance against a particular regulatory requirement, it does provide confidence that business continuity is a discipline with measurable outputs. It also helps to provide assurance to suppliers and customers that resilience is taken seriously within an organization and is a safe organization to do business with.

The more specific needs for accreditation against regulatory requirements in banking, healthcare, government, securities, and some other sectors will, of course, provide the most important approval for regulated firms to achieve. Beyond regulated firms, some will define resilience as an overarching framework with business continuity as a specialization within it. Other firms will adopt the approach often taken in financial services with business continuity and operational resilience being complementary.

Business continuity managers have tended to concentrate on practical matters such as developing plans, validating those plans through exercising, and providing knowledge-based practical support during an invocation. They have become the internal subject matter experts and often manage the central support for any tools or technology involved in resilience processes. This has traditionally made their role vital but not fully integral to the running of the business. However, this has changed in organizations where business continuity is now part of the supplier compliance process. Not only do they have to be able to demonstrate to prospective customers that their own company is properly protected, but they also need to be able to evaluate potential suppliers plans and processes for the quality of their business continuity.

This expansion of the role is positive for business continuity practitioners. It means business continuity can become an even more important part of the organization, and business continuity managers will have more interesting and challenging jobs with wider career opportunities.

The technical component of business continuity has grown since COVID-19, and business continuity professionals have needed to expand their technical skills to support hybrid working, video conferencing, emergency communication tools, AI-powered resilience tools, and/or supply chain mapping tools. Acquiring and using tools – such as emergency communications software, crisis management simulation and monitoring, and new AI-technology – is providing an enhanced career path for business continuity professionals.

AI is set to transform processes within business continuity teams. Data analytics, scenario design, simulations, and forecasting are ideal candidates for its use. It does still need to be used with care, however. While AI can help to optimize the BC process, humans will still need to provide the final review and ensure the source data is clean and correct. Ultimately, practitioners will be able to spend more time carrying out other elements of their role like building cross functional relationships, interviewing, running exercises, planning response strategies, and coordinating invocations. However, it will take some time for practitioners to become comfortable with mass adoption of AI in business continuity programs.

Take Aways

1. The top five risks remain the same as for the previous year. Since the end of the COVID-19 pandemic these five risks – cyber events, IT disruptions, adverse financial conditions, natural disasters, and HR issues – have dominated the rankings.
2. The most important risk over the past decade has been cyber-attacks in various forms, as well as concerns over our ability to maintain effective cybersecurity. This is an ongoing and expanding challenge in which business continuity, cybersecurity and IT need to work closely together.
3. Despite the relatively recent experiences with COVID-19, the risk from infectious diseases does not rank highly as a current concern. This is despite new COVID strains and other diseases which could potentially become epidemics being monitored by the World Health Organization. This may indicate an overconfidence in our ability to survive future pandemics.

4. Supply chain disruptions remain a significant concern, despite attempts of many firms to diversify their sources of supply following COVID-19 experiences. Attempts to reduce the negative impact of globalization by more local sourcing and the reintroduction of onshoring and nearshoring for manufacturing reduces risk but is complicated, lengthy, and costly.
5. AI can provide huge benefits to organizations, but it comes with risk. It is still relatively new, and problems emerge when AI results are presented as fact, without testing or validation. AI has significant potential for business continuity by simplifying the planning and administration work, thus allowing more time to focus on relationship building.
6. Business continuity can benefit from both AI and the growth of a resilience culture. It has a unique skillset and knowledge base which should make it a central player in responding to any type of emergency or crisis. However, for this to be fully effective, board-level executives need to ensure a resilient culture flows from the top to the base of an organization.

Appendix

The PROBABILITY of the risk occurring

Rank	Icon	Issue	Average Value
1		Cyber events	4.03
2		IT disruptions	3.73
3		Financial conditions	3.53
4		Natural disasters	3.19
5		HR issues	3.13
6		Climate change	3.01
7		AI issues	2.98
8		Supply chain disruptions	2.98
9		Power shortages	2.92
10		Increased regulation	2.90
11		Reputational issues	2.88
12		Major facility incident	2.86
13		Infectious diseases	2.74
14		Civil unrest	2.70
15		Terrorism	2.35

The BUSINESS IMPACT if the risk occurs

Rank	Icon	Issue	Average Value
1		Cyber events	4.15
2		IT disruptions	3.95
3		Financial conditions	3.51
4		Natural disasters	3.32
5		Reputational issues	3.30
6		Power shortages	3.26
7		Major facility incident	3.21
8		HR issues	3.13
9		Increased regulation	3.09
10		Supply chain disruptions	3.06
11		AI issues	3.05
12		Infectious diseases	2.95
13		Terrorism	2.88
14		Climate change	2.86
15		Civil unrest	2.76

End Notes

[1]https://www.theguardian.com/world/article/2024/jul/19/taiwan-semiconductor-industry-booming

[2]https://journals.sagepub.com/doi/10.1177/19401612241311886

[3]https://www.independent.co.uk/news/business/chris-bryant-jaguar-land-rover-tata-motors-gavin-williamson-minister-b2823113.html

[4]https://industrialcyber.co/regulation-standards-and-compliance/house-republicans-reintroduce-bill-to-counter-chinese-cyber-threats-to-critical-infrastructure/

[5]https://www.forbes.com/sites/alexvakulov/2025/03/09/deepfake-scams-are-stealing-millions-how-to-spot-one/

[6]https://sourceability.com/post/the-limitations-of-renewable-energy-in-the-face-of-growing-data-center-power-demands

[7]https://www.ecoflow.com/za/blog/rolling-blackout

[8]In addition, a category "other" was added and includes Africa, Australia, New Zealand, and some small island nations.

[9]https://www.pwc.nl/en/insights-and-publications/themes/economics/25th-ceo-survey/ceos-are-most-concerned-about-cyber-risks.html

[10]https://www.cbsnews.com/news/most-violent-conflicts-since-world-war-ii-un-says/

[11]https://www.ndtv.com/world-news/world-saw-highest-number-of-armed-conflicts-in-2024-since-1946-study-8642241

[12]https://www.climatecouncil.org.au/resources/2024-marks-worlds-worst-heat-climate-pollution/

[13]https://www.bbc.co.uk/weather/articles/c1el8z2d7v8o

[14]https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[15]https://www.esgdive.com/news/sec-rules-banks-cant-exclude-climate-social-shareholder-proposals-jpmorgan-citi-bofa-wells-ms/742591/

[16]https://www.sciencedirect.com/science/article/pii/S0007681325000370

[17]https://www.stlouisfed.org/on-the-economy/2025/aug/recent-college-grads-bear-brunt-labor-market-shifts

[18]https://www.esgdive.com/news/sec-rules-banks-cant-exclude-climate-social-shareholder-proposals-jpmorgan-citi-bofa-wells-ms/742591/

[19]https://rollingout.com/2025/06/22/signs-banks-might-abandon-esg-investing/

[20]https://www.sciencedirect.com/science/article/pii/S0007681325000370

[21]https://committees.parliament.uk/work/8823/government-cyber-resilience/news/206712/cyber-threats-government-defences-have-been-outpaced-by-hostile-states-and-criminals/

[22]https://www.news-medical.net/news/20250613/WHO-warns-of-ORVO-as-outbreaks-surge-and-health-risks-rise.aspx

[23]https://www.nationalgeographic.com/science/article/141119-ebola-dengue-chagas-chikungunya-tropical-diseases-health

[24]https://hbr.org/2024/03/lessons-from-the-bud-light-boycott-one-year-later

[25]https://www.bbc.co.uk/news/articles/c0el31nqnpvo

[26]https://news.sky.com/story/mands-tech-chief-leaves-months-after-cyberattack-cost-it-300m-13428656

The 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 and Chief Knowledge Officer for DRI International. 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. Bird is currently Editor of the Journal of Business Continuity and Emergency Planning, a member of the Advisory Board for the Crisis Management Response Journal, and a regular contributor to the US based Resilience Hub platform.

Patrick Alcantara is head of strategic customer insight at AXA UK, and has worked for other well-loved British brands such as Co-op Insurance and O2. He was also the former head of research at the Business Continuity Institute (BCI), where he extended the resilience industry's evidence base by introducing new reports on climate change, cyber resilience, emergency communications, salary benchmarking, and the future of the industry, among others. He has also delivered research on behalf of organizations such as the former UK Department of Business, Innovation & Skills, BSI, Everbridge, PwC, SAP, Siemens Netherlands, Sungard AS, and Zurich Insurance. He specializes in harnessing customer data, using foresight, and conducting quantitative/qualitative research to support customer, commercial and regulatory outcomes. He also serves on the editorial board of the Journal of Business Continuity and Emergency Planning and holds a Business Continuity Management diploma and an Executive Data Science credential. He has been interviewed and has spoken at podcasts and conferences in various countries including the Czech Republic, Germany, the Netherlands, the Philippines, Switzerland, the UK, and the US.

Alcantara brings more than 15 years of experience in quantitative/qualitative research, market intelligence, and business analytics. He also holds an Executive Data Science credential and a Diploma in Business Continuity Management. Alcantara has a bachelor's in psychology and a master's degree with Distinction from the Institute of Education (University College London). He is currently based in the United Kingdom.

Dr.Yair Amir, PhD, is Professor Emeritus of Computer Science, and Director of the Distributed Systems and Networks Lab at Johns Hopkins University. His goal is to invent resilient, performant, and secure distributed systems that make a difference, collecting friends along the way.

Amir served as Professor (1995-2023) and Department Chair (2015-2018) of Computer Science at Johns Hopkins, as program co-chair (2015) and general co-chair (2022) of the IEEE/IFIP Dependable Systems and Networks (DSN) conference, and as a Vice Chair of the IFIP 10.4 Working Group on Dependable Computing (2016-2018). He is a member of the National Academies' Forum on Cyber Resilience since 2019.

Amir is a co-founder of Spread Concepts LLC, a consulting company helping clients with the design, development, and deployment of resilient infrastructure systems.

Amir is a co-founder and Chief Science Officer of LTN Global Communications, a cloud service provider offering live video transport and processing services that are used by major media companies including Disney, YouTube TV, CNN, Fox, ABC, BBC, Bloomberg, CBS, Deutsche Welle, ESPN, NBC, PBS, and Turner.

Amir holds BSc (Summa Cum Laude) and MSc from the Technion, Israel Institute of Technology, and a Ph.D. from the Hebrew University of Jerusalem, Israel.

Al Berman, MBCP, CBCLA, CCRP, is Treasurer and Board Member of DRI International, and the President of the DRI Foundation. During his career, Berman has been President of a major US bank subsidiary, CIO for a major trust company, National Practice Leader for Operational Resiliency (PricewaterhouseCoopers), Global Business Continuity Management Practice Leader (Marsh), and Program Director for BCM for a major healthcare organization.

Berman has served on the Homeland Security Standards Panel, US congressional committee Project on National Security Reform, ANSI-ANAB Council of Experts, NYC Partnership for Risk Management and Security, and Chair for the Alfred P. Sloan Foundation committee to create the new standard for the US Private Sector Preparedness Act (PS-Prep). He has worked with governments in the US, Middle East, Latin America, and Asia to create standards and regulations.

His career in cybersecurity spans 4 decades, from being part of a US government tiger team vested with the responsibility of finding flaws in networks and systems, to creating security systems used by IBM and other major system developers, to serving on government committees. Berman serves as an adviser to companies and governments worldwide on issues including resilience, business continuity, disaster recovery, geopolitical risk, and cybersecurity. Berman's articles and interviews have been on TV, radio, printed media, and online publications around the world.

Dr. Ray Chang, Ph.D., is a tenured associate professor in The Department of Security and Emergency Services at Embry-Riddle Aeronautical University-Worldwide. Before he pursued his doctoral degree, he was in charge of developing emergency operations plans for high-rise buildings, subway stations, and the longest tunnel (8 miles) in Taiwan. Chang earned his M.S. in Fire Service Administration from Arizona State University and his Ph.D. in Disaster Science and Management from the Biden School of Public Policy and Administration at the University of Delaware.

Chang's research areas include disaster preparedness, disaster response, and fire service administration. He is a principal member of the National Fire Protection Association (NFPA) 1600 (Standards on Continuity, Emergency, and Crisis Management) code development committee. He also serves as a subject matter expert for several governmental agencies in Taiwan (e.g., the Office of Homeland Security and Taipei City Government) to increase their capabilities of disaster preparedness and response.

Linda Conrad is the Senior Vice President responsible for global Enterprise IT Risk Management, Innovation, Business Continuity, Compliance, Security Architecture, Security Operations, Identity and Access Management, Security Engineering, Data Protection, and Education for information security and technology across Everest Re Group. She develops and implements strategies to protect Everest's global technology, proprietary data, and digital ecosystem with the goal of supporting global expansion and organizational transformation.

Conrad previously worked as Principal, Corporate and Information Security Services for Exelon Corporation. She helped develop a dynamic dashboard process and implemented a business intelligence tool to support corporate, cyber and Third-Party Key Performance and Risk Indicators. Conrad managed Background Investigations Services, where she launched an International Risk Mitigation Process across all Exelon Operating Companies

Prior to Exelon, Conrad was the Director of Strategic Business Risk at Zurich, where she founded and headed a global team responsible for developing and delivering a Strategic Risk Management product suite. She also served as interim CEO of a start-up, where she led a team which pioneered innovative financial and technology products.

Conrad partnered with National Institute of Standards and Technology on creation and predictive analytics for a cyber supply chain risk portal, which received the Cybersecurity Award for Practice from Institute of Electrical and Electronics Engineers. She addresses enterprise resiliency issues in print and television appearances, including CNBC, Fox Business News, The Financial Times, and The Wall Street Journal. Conrad is an Adjunct Professor of Supply Chain at Robert H. Smith School of Business and holds a Specialist Designation from Institute of Risk Management in London.

Rachael Elliott is Director of Global Strategy and Innovation for DRI International. Prior to joining the DRI, Elliott led the Thought Leadership department at the Business Continuity Institute (BCI) for six years. Prior to that, she has nearly 20 years' experience leading commercial research in organizations, such as HSBC, BDO LLP, Marakon Associates, CBRE, and BCMS. She has particular expertise in the technology side of resilience, and has a keen interest in how artificial intelligence can help to transform the resilience of organizations. Her research has been used in the UK Parliament to help develop government industrial strategy as well as in the BDO High Street Sales Tracker, which Elliott was instrumental in developing and is still the UK's primary barometer for tracking high street sales performance. She maintains a keen interest in competitive intelligence and investigative research techniques.

Boris Issavi, CBCP, MBCP, CBCV, is an experienced leader in risk and business continuity management and related disciplines (i.e. security operations, crisis/incident management, disaster recovery). He is the Director of Business Continuity Management Program at Gilead Sciences Responsible for its overall BCM program, aiming at increasing enterprise resiliency and reducing risk exposure. In his current role, Issavi manages all phases of planning, analysis, and implementation of recovery solutions in direct support of resilience and crisis management objectives from the conceptual stage to the final execution. He has implemented resiliency strategies both, from ground-up or from an existing program to the next level of maturity. He is the corporate liaison on Physical Climate Risk Assessment for the Task Force on Climate-related Financial Disclosures (TCFD) framework.

Issavi works hand in hand with business partners at various affiliates worldwide on strategic and operational roadmaps that are aligned with the company's risk profile, and partners with the Sustainability Group on Physical Climate Risk Assessment initiatives, as well as working closely

with Enterprise Risk Management (ERM) within the Audit group, Facilities Operations on crisis management and planning, and IT Security on systems' disaster recovery.

He serves as business continuity and enterprise risk management (BC/ERM) track lead for mergers and acquisitions (M&A), and serves as BCM function lead on incident assessment and incident response teams (IAT & IRT) at the enterprise level.

Prior to Gilead, Issavi systematically built his expertise in operational risk over 20 years, mainly in the financial, healthcare, and pharmaceutical industries. As a leader, he strives to create an environment where ideas can flourish, and effective solutions materialize.

Richard Knowlton is Director of Security Studies at the Oxford Cyber Academy and Visiting Lecturer at the Cambridge Judge Business School. He is 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.

Steven Lei, CBCP, is an organizational change and risk management leader with over 15 years of cross-functional experience in the public, private, and non-profit sectors. He is currently Assistant Vice President of Business Continuity and Disaster Recovery at East West Bank, a publicly traded bank with over 120 locations in the U.S. and Asia. Previously, Lei has held strategic roles in finance and business operations at the Federal Reserve Bank and the University of California System, and served as a business resilience consultant at Facebook.

In 2023, Lei was appointed to serve on the Los Angeles County Economy and Efficiency Commission. Previously, he served on the San Francisco Civil Grand Jury, a state constitutionally-mandated body responsible for examining the conduct and operations of county government. His current and previous board service includes Opera Parallèle, the Pony Barnes Foundation (LGBTQ+ and educational focused grant maker), BluPeak Credit Union ($1B+ in assets); the Institute of Human Behavior, Research, and Education, and the Chinese Historical Society of America Museum.

Lei earned his Bachelor's degree at the University of California, San Diego, Master's degree at the London School of Economics, and has completed the Accelerated Management Program at the Yale School of Management. In addition to his CBCP designation with DRI, he is certified as a Community Emergency Response Team (CERT) volunteer, and holds the Society for Human Resource Management's Senior Certified Professional credential (SHRM-SCP).

Eric J. McNulty holds an appointment as Associate Director for the Program for Health Care Negotiation and Conflict Resolution and at the National Preparedness Leadership Initiative, a joint program of the Harvard Chan School and the Harvard Kennedy School of Government. He is an Instructor at the Harvard T.H. Chan School of Public Health. His work centers on leadership in high-stakes, high-stress situations. McNulty's most recent book, You're It: Crisis, Change, and How to Lead When it Matters Most (Public Affairs, 2019) is based on meta-leadership, the core leadership framework of the group's curriculum. He teaches in graduate-level courses on public health leadership, conflict resolution, and negotiation as well as serving as Program Co-director for the Leading in Health Systems executive education program at the Chan School. He also teaches in executive education programs at Harvard Medical School, MIT, and UC San Diego Health.

McNulty is the co-author, along with Dr. Leonard Marcus and Dr. Barry Dorn, of the second edition of Renegotiating Health Care: Resolving Conflict to Build Collaboration (Jossey-Bass, 2011). He is the principal author of case studies on leadership decision making in the Boston Marathon bombing response, innovation in the response Hurricane Sandy and the professional/political interface in the Deepwater Horizon response drawing upon his first-hand research as well as extensive interviews with leaders involved in the responses. McNulty has written more than 200 by-lined articles for the Harvard Business Review (HBR), Sloan Management Review, Strategy+Business, and other publications as well as several for peer-reviewed journals. His HBR cases have been anthologized through the HBR paperback series and have been used in business education curricula in the United States and as far away as France and the Philippines.

David Porter was the Director of Business Continuity Management (BCM) at the Australian Taxation Office (ATO) from September 2010 and has provided a strategic oversight role since August 2016, while leading technology, HR and building refurbishment projects.

Porter developed the Australian whole-of-government BCM Community of Practice, with members from over 40 Commonwealth and state-based agencies. He provides regular mentoring support for other organisations locally and has represented the ATO in London, Berlin and Jakarta. As a member of several forums, Porter has contributed towards the emergency readiness and preparedness across the public sector and finance industries. As well as leading several national level responses to business interruptions and natural disasters, Porter has guided senior executive and board level groups through detailed crisis simulation testing and exercises.

Porter has established a credible, international profile within the BCM industry, through his work with the Disaster Recovery Institute's Future Vision Committee and regularly presenting at national and international conferences. He has been published in the peak industry academic publication Journal of Business Continuity and Emergency Planning and forms part of the global editorial board with 25 other industry leaders.

Porter has received several national and international awards across continuity and risk related industries. He has also worked with the United Nations Office of Disaster Risk Reduction to benchmark effective organizational responses to natural disaster events. Porter has completed studies in Business Management and holds a Bachelor of Digital Design from Curtin University.

Dr. Kenji Watanabe is a professor at the Graduate School of Social Engineering, and also the head of Disaster & Safety Management of the Nagoya Institute of Technology, with major research areas in risk management, business continuity management (BCM), and critical infrastructure protection (CIP). He has almost 20 years of business experience at the Mizuho Bank, PricewaterhouseCoopers, and IBM Business Consulting Services in financial business and risk management fields.

He is also a chair or a professional member of several Japanese governmental committees at the Critical Infrastructure Protection Council (Cabinet Secretariat), the Food Security Advisory Board (Ministry of Agriculture, Forestry and Fisheries), the Transportation Safety Council (Ministry of Land, Infrastructure, Transport and Tourism), and others. As international activities, he is a member of the DRI Future Vision Committee, the head of delegates of Japan for ISO/TC292(Security and resilience), editorial committee member of the International Journal of Critical Infrastructure Protection (IJCIP) and the Journal of Disaster Research (JDR).

He has executed many disaster management related projects including the Area-BCM project in Thailand sponsored by JICA to enhance regional disaster resilience at industry complexes. (2017-2024). He holds PhD (Waseda University) and MBA (Southern Methodist University).

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 20,000+ resilience professionals in 110+ 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 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