Global FINEX - Directors and Officers Insurance (D&O)

Directors' Liability Survey 2022

April 2022

wtwco.com

Contributors

CLYDE&CO

Richard Berkahn
Partner, Sydney
+61 2 9210 4981
richard.berkahn@clydeco.com

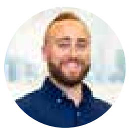
Mark Beswetherick
Partner, Dubain
+971 4 384 4000
mark.beswetherick@clydeco.com

Ian Birdsey
Partner, London
+44 20 7876 6272
ian.birdsey@clydeco.com

Patrick Boardman
Partner, London
+44 20 7876 6272
patrick.boardman@clydeco.com

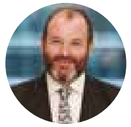
Dean Carrigan
Partner, Syndey
+61 2 9210 4401
dean.carrigan@clydeco.com

Alec Christie
Partner, Sydney
+61 2 9210 4510
Alec.Christie@clydeco.com



Reece Corbett-Wilkins
Partner, Syndey
T: +61 2 9210 4984
E: reece.corbett-wilkins@clydeco.com

Laura Cooke
Partner, London
T: +44 20 7876 6387
E: laura.cooke@clydeco.com



James Cooper
Partner, London
T: +44 20 7876 6388
E: james.cooper@clydeco.com

Ignacio Figuerol
Partner, Madrid
+34 91 793 45 01
iIgnacio.figuerol@clydeco.com

Chris Holme
Partner, London
+44 20 7876 6216
Chris.Holme@clydeco.com

Jacques Jacobs
Partner, Sydney
+61 2 9210 4448
Jacques.Jacobs@clydeco.com

Edward (Ned) Kirk
Partner, New York
+1 212 710 3960
edward.kirk@clydeco.us

Avryl Lattin
Partner, Sydney
T: +61 2 9210 4425
E: avryl.lattin@clydeco.com

Sumeet Lall
Partner, New Delhi
+91 11 4005 4550
sumeet.lall@cslchambers.com

Daniel Le Roux
Partner, Johannesburg
+27 10 286 0357
daniel.leroux@clydeco.com

Lucinda Lyons
Partner, Sydney
+61 2 9210 4497
lucinda.lyons@clydeco.com

Simon McConnell
Managing Partner
+852 2287 2723
simon.mcconnell@clydeco.com

David Mehut
Partner
+33 1 44 43 89 85
David.Meheut@clydeco.fr

John Moran
Partner, Sydney
T: +61 2 9210 4974
E: john.moran@clydeco.com

Rosie NG
Partner, Singapore
+852 2287 2748
rosie.ng@clydeco.com

Contributors

CLYDE&CO


Jane O'Reilly
Associate, London
+44 20 7876 5468
jane.oreilly@clydeco.com


Mandip Sagoo
Partner, London
+44 20 7876 4661
mandip.sagoo@clydeco.com


Dr Henning Schaloske
Partner, Dusseldorf
+49 211 8822 8800
henning.schaloske@clydeco.com


Christopher Smith
Partner, Sydney
T: +61 2 9210 4493
E: christopher.smith@clydeco.com


Jacinta Studdert
Partner, Sydney
T: +61 2 9210 4930
E: jacinta.studdert@clydeco.com


Nicholas Skyes
Partner, Singapore
+65 6544 6533
nicholas.sykes@clydeco.com


Mark Sutton
Partner, London
T: 44 20 7876 6256
E: mark.sutton@clydeco.com


Alena Titterton
Partner, Sydney
+61 2 9210 4577
alena.titterton@clydeco.com


Marc Voses
Partner, New York
+1 212 710 3968
marc.voses@clydeco.us


Mun Yeow
Partner
+852 2287 2722
mun.yeow@clydeco.com

Contributors

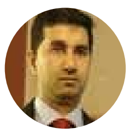
Elizabeth Adamson
FINEX Canada - Commercial Practice Leader
+1 416 960 7133
elizabeth.adamson@willistowerswatson.com

Angus Duncan
Global D&O Coverage Specialist (ex NA)
+44 20 3124 8386
angus.duncan@willistowerswatson.com

Lawrence Fine
Management Liability Coverage Leader
FINEX North America
+44 20 3124 7999
larry.fine@willistowerswatson.com

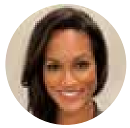
Graeme Griffiths
Financial Lines Leader - South Africa
+27 0 81 864 8175
graeme.griffiths@willistowerswatson.com

Ulysses Grundey
Director
+34 911 54 97 16
ulysses.grundey@willistowerswatson.com



Namit Mahajan
Head of FINEX Asia
+65 6958 2764
namit.mahajan@willistowerswatson.com

Richard Multon
Head of Broking, Commercial D&O
T: +44 203 124 6459,
richard.multon@willistowerswatson.com



Joann Nilsson
Claims Advocate
+1 212-915-8388
joann.nilsson@willistowerswatson

John M. Orr
D&O Liability Product Leader, FINEX NA
+1 415 745 2681
John.Orr@WillisTowersWatson.com

Jill Stewart
Head of FINEX (Financial & Executive Risks) Australasia
+ 61 2 9285 4091
jill.stewart@willistowerswatson.com

Timothy Sullivan
Asset Management Industry Leader
+1 7 3167 8516
timothy.sullivan@willistowerswatson.com

Glyn Thoms
Head of G.B. FINEX Cyber & TMT
+ 44 20 3124 8673
glyn.thoms@willistowerswatson.com

Eve Richards
G.B. Head of FINEX D&O
T: +44 20 3124 6459,
eve.richards@willistowerswatson.com

Jon Vocking
Head of U.K. D&O
+44 203 124 8885
jon.vocking@willistowerswatson.com

Marcela Visbal Acuña
Regional Cyber Product Leader,
Latin America
+ 57 1 742 4001 Ext. 1627
marcela.visbal@willistowerswatson.com

Robert Weaver
Account Director, New Zealand, FINEX
+ 64 21 909 541
robert.weaver@willistowerswatson.com

Directors' Liability Survey 2022

April 2022

Table of contents

Introduction

Welcome to the 2022 Directors Liability Survey Report from WTW in partnership with Clyde & Co LLP. Last year, we produced our first international survey report. This year, we have expanded the scope with responses from directors and risk managers based in more than 40 countries around the world. As a result, we can now compare results from G.B., the U.S., Latin America, Europe, Asia and Australia.

We have also enhanced the survey to include:

- More questions regarding climate change risk for directors focusing down on the different aspects of physical risk, transition risk and risks arising from climate change reporting requirements.
- A further cyber-related risk: cyber extortion. This risk provoked a strong response from respondents, immediately becoming a Top 5 risk across all regions (see the article [Cyber Extortion - ransomware and payment of ransoms] on page 36).
- Questions exploring to what extent the respondents' businesses have implemented captive insurance vehicles or other alternatives to the commercial D&O insurance markets.

Some interesting results have emerged from the new questions. Despite the increased attention on climate change risks following COP26 and recent regulatory changes, it still remains outside the top 5 risks in any region. However, it has risen to be the number six risk for directors in G.B., Asia and Australasia and when looked at by industry grouping, climate change does make it into the top 5 for finance and insurance, as well as for energy & utilities (see the article [Climate change, environment and other ESG factors] on page 37.

Our question regarding the use of "captives" and alternative risk transfer solutions highlighted that up to 20% of respondents said that their businesses were considering implementation of alternatives in the future and the highest of the implemented alternatives was a personal guarantee of directors liabilities from a CEO, major shareholder or other source (see further our article [Use of alternatives to the commercial insurance market for D&O liabilities] on page 56.

The increased international scope of the survey allows for interesting comparisons of the regional responses. One particular area where this can be seen is in the D&O insurance limits being purchased by the respondents' businesses. In LatAm, we can see that 19% purchased no D&O insurance compared with 0-8% for respondents across the other regions. By contrast, 28% of respondents in Europe and 31% of respondents in North America purchased €/$100+ million. We consider the D&O insurance aspects further in our article [Directors and officers insurance coverage] on page 47.

Given the international nature of the responses to this survey, in addition to articles covering specific topics, we have also included for the first time regional overviews (see pages 14-18) as well as a review of the overall top 5 risks, kindly undertaken by James Cooper at Clyde & Co (see article [Top 5 risks] on page 13).

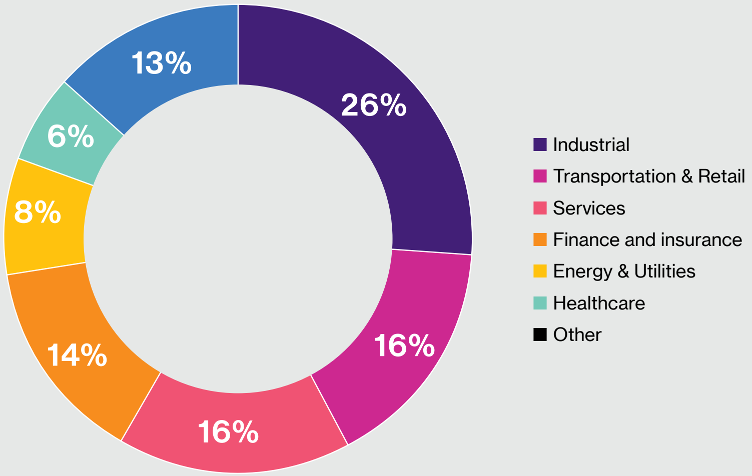
The report only touches the surface of the data which we have collected and should you wish any further information, please do get in touch. Similarly, if you have any suggestions for topics or questions to be included in our next Directors' Liability Survey, please let us know. We hope that you find the report interesting.

Finally, we would like to thank everyone around the world who took the time to complete our survey and, of course, to the many colleagues from WTW and our partners, Clyde & Co, for all of the efforts that they have put into analysing the survey responses and contributing to this report.

Angus Duncan
Global D&O Coverage Specialist (ex NA)
+44 20 3124 8386
angus.duncan@willistowerswatson.com

Key findings

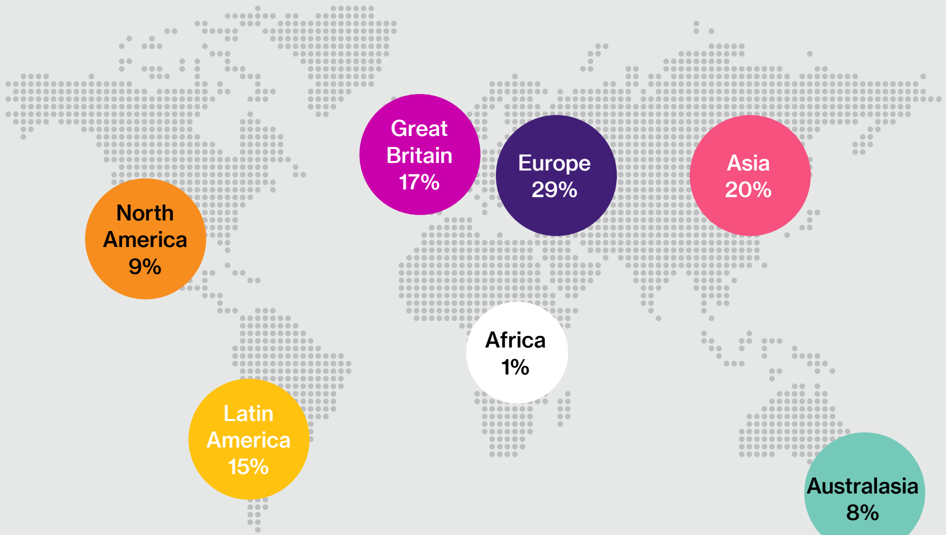
Industry distribution



Note: Revenues in EUR, GBP, JPY and CNY were converted to USD with rates as of November 9, 2021. Percentages may not add up to 100% due to rounding.

Source: Directors' Liability Survey 2022

Responses by country

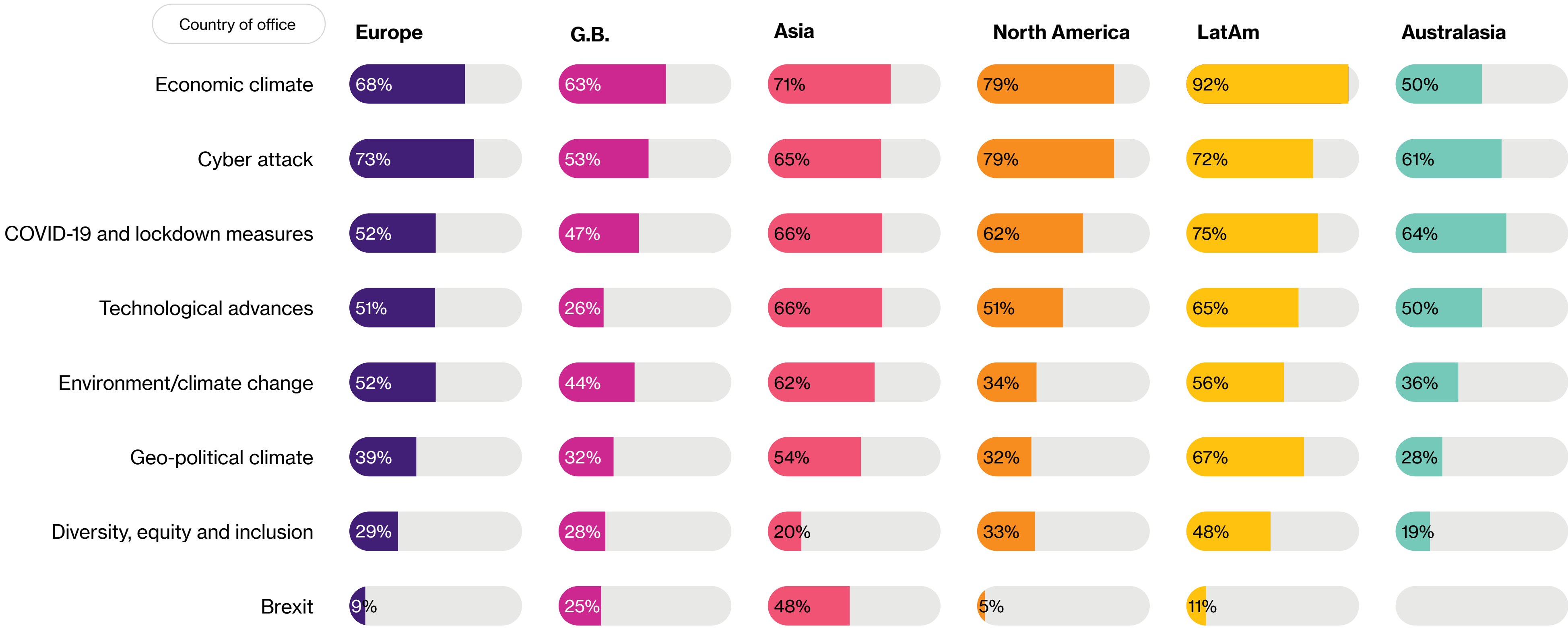


Note: Percentages may not add up to 100% due to rounding

Source: Directors' Liability Survey 2022

Risk to business operations – by region

How significant do you think each of the following risks are to you or your business?



(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Top 5 risks to directors

	2018	2019	2021	2022
1	Risk of data loss / data breach ▲	Data loss ►	Cyber attack ▲	Cyber attack ►
2	Cyber attack ►	Cyber attack ►	Data loss ▼	Data loss ►
3	Regulatory and other investigations ▼	Regulatory risk (including threat of fines and penalties) ▲	Regulatory risk (including threat of fines and penalties) ►	Cyber extortion ▲
4	Health and safety legislation ▲	Litigation risk ▲	Risk of a health and safety / environmental prosecutions safety legislation ▲	Regulatory risk (including threat of fines and penalties) ▼
5	Criminal and regulatory fines and penalties ▼	Your company becoming a focus of a social media campaign ▲	Risk of employment claims ▲	Risk of a health and safety / environmental prosecutions safety legislation ▼

▲ Risk ranking has increased for D&O'S

▼ Risk ranking has decreased for D&O's

► Risk ranking has remained the same for D&O's

Note: Ranked based on percentage very or extremely important for each risk

Source: Directors' Liability Survey 2022

Risk ranking overview – historical comparison

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)?

		2019	2021	2022
Cyber	Cyber attack	54%	56%	65%
	Data loss	55%	49%	63%
	Cyber extortion			59%
Legal	Regulatory risk (including threat of fines and penalties)	50%	46%	49%
	Shareholder actions/disputes		27%	36%
	Anti-trust law/regulation	38%	26%	29%
Operational	Risk of a health and safety / environmental prosecutions	38%	41%	46%
	Return to work/COVID-safety/vaccination status			35%
	Risk of employment claims		38%	35%
	Risks posed by supplier business practices	38%	27%	34%
	Breach of human rights within your business operations	32%	23%	32%
	Board/ management/ company takeover or other forms of activism by shareholders or institutional investors			27%
Crime	Economic crime (your company/organisation as a victim)	38%	29%	39%
	Bribery and corruption	34%	27%	39%
	Risk of criminal penalties arising from breach of sanctions	35%	29%	38%
	Social engineering crime (your organisation as a victim)			37%
	Risk of other criminal proceedings	37%	22%	29%
Environmental & Social	Climate change			38%
	Your company/organisation becoming a focus of a social media campaign		30%	36%
Financial	Insolvency, bankruptcy or corporate collapse	38%	26%	31%
Jurisdiction	Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	37%	25%	26%
Pension	Pensions liabilities		24%	20%

(% of 'Very significant' or 'Extremely significant'

Source: Directors' Liability Survey 2022

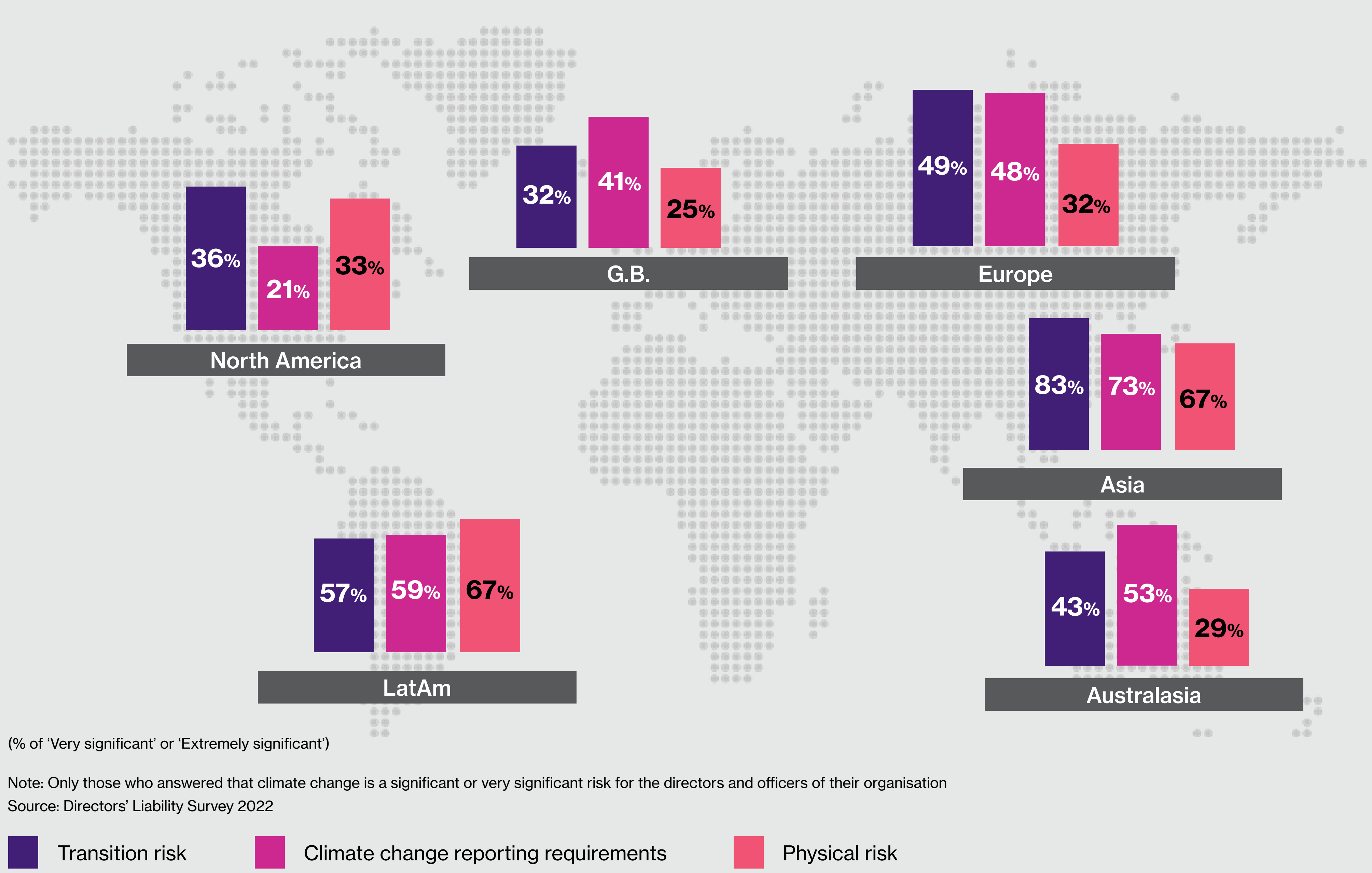
Risk ranking overview – regional comparison

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)?

Country of office	Europe	G.B.	Asia	LatAm	North America	Australasia
Cyber attack	71%	47%	70%	64%	77%	57%
Data loss	65%	43%	70%	62%	86%	46%
Cyber extortion	63%	36%	63%	54%	80%	46%
Regulatory risk (including threat of fines and penalties)	46%	35%	64%	31%	75%	32%
Shareholder actions/disputes	36%	11%	51%	18%	73%	6%
Anti-trust law/regulation	34%	10%	42%	18%	38%	12%
Risk of a health and safety / environmental prosecutions	46%	40%	48%	15%	67%	41%
Return to work/COVID-safety/vaccination status	25%	11%	51%	38%	68%	20%
Risk of employment claims	28%	14%	50%	31%	67%	14%
Risks posed by supplier business practices	23%	13%	61%	33%	62%	11%
Breach of human rights within your business operations	28%	8%	52%	10%	66%	11%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	24%	8%	53%	13%	44%	6%
Economic crime (your company/organisation as a victim)	38%	13%	49%	23%	75%	26%
Bribery and corruption	42%	13%	56%	10%	74%	9%
Risk of criminal penalties arising from breach of sanctions	37%	15%	51%	18%	69%	21%
Social engineering crime (your organisation as a victim)	32%	14%	48%	36%	69%	17%
Risk of other criminal proceedings	32%	10%	44%	10%	50%	6%
Climate change	34%	24%	58%	18%	52%	31%
Your company/organisation becoming a focus of a social media campaign	33%	22%	46%	24%	63%	22%
Insolvency, bankruptcy or corporate collapse	33%	10%	42%	3%	67%	8%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	27%	10%	45%	3%	42%	9%
Pensions liabilities	19%	11%	24%	13%	42%	3%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Climate change – by region



(% of 'Very significant' or 'Extremely significant')

Note: Only those who answered that climate change is a significant or very significant risk for the directors and officers of their organisation
Source: Directors' Liability Survey 2022

Top five directors and officers risks

James Cooper, Clyde & Co

It is, perhaps, no surprise respondents identified their top two risks to directors to be cyber attacks and data loss, those having topped the list for the last three years.

However, making a new entry is cyber extortion. The past year saw attacks evolve from attackers simply encrypting data to encryption and exfiltration, also known as double extortion and, further, into triple extortion, where the attackers seek to extract money from third parties related to the initial breach, such as customers. This is a worrying development and adds a further level of pressure on directors and officers to implement adequate cybersecurity controls and to react efficiently and effectively in the face of an attack.

Cyber risk is a multi-varied and ever-evolving risk, with a variety of significant consequences should an attack occur and data is lost, making cyber risks of primary concern. Regulatory/administrative data protection fines have increased in volume and scale and while the English courts have sought to limit the scope of damages for immaterial losses, there is an evolving body of case law on a European level in terms of a company's liability in this regard and an increasing risk that insufficient engagement with cyber issues poses a liability risk for directors and officers on many fronts, including class actions.

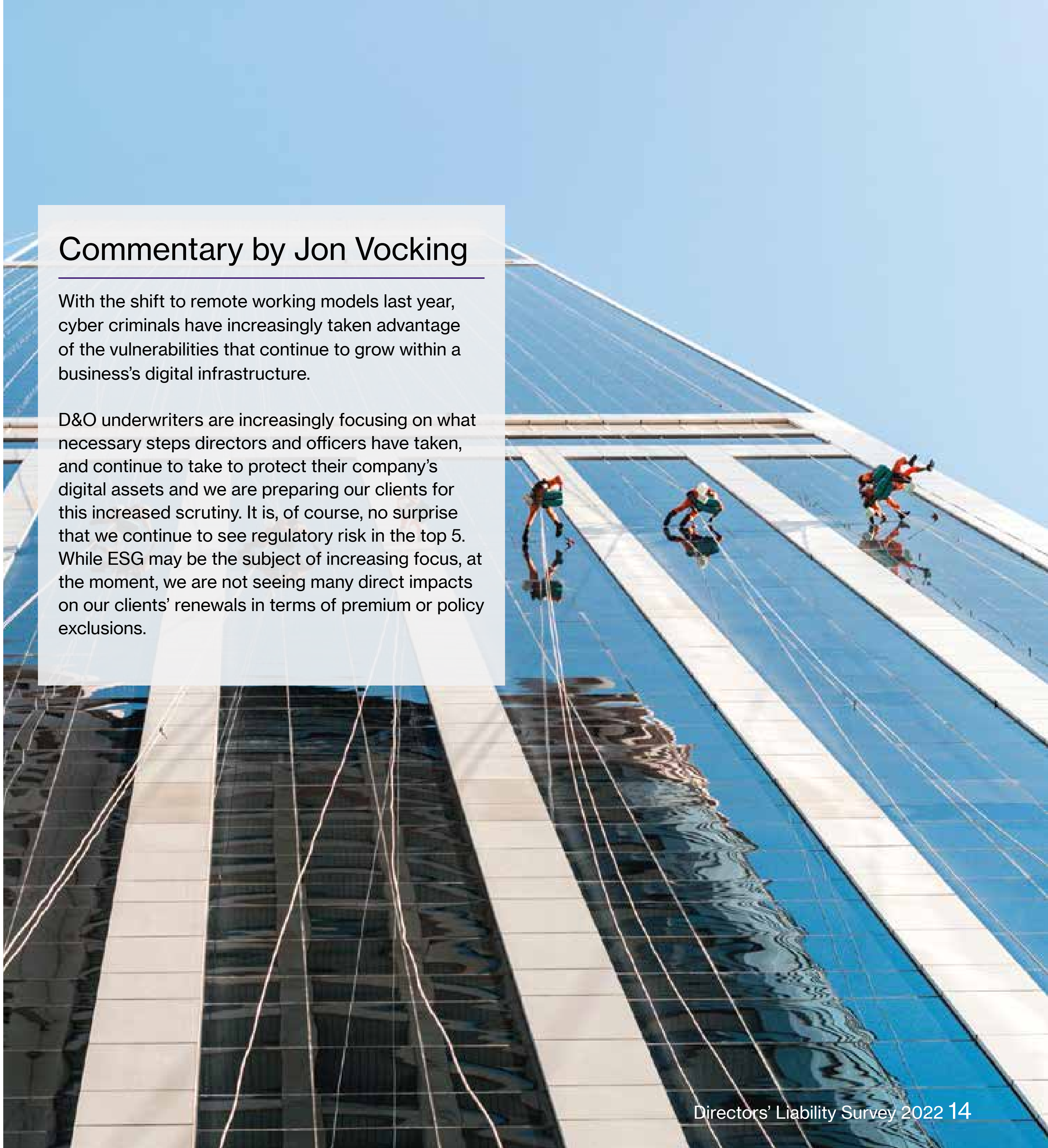
Regulatory risk, including the threat of fines and penalties, remains high on the list of concerns, with Asia and LatAm expressing the highest level of concern and the financial sector feeling most exposed. Following slight dips in activity throughout 2020 and into 2021, regulators have rebounded in many jurisdictions and often with a stronger focus on systems and controls, operational resilience and protection of consumers, given the gaps identified in many organisations when the pandemic hit.

Those failings are expected to translate into enforcement actions in due course. This sits alongside growing regulatory compliance requirements, a continued focus on traditional risks, such as money laundering and market abuse, plus emerging areas of focus, such as cryptocurrencies.

Rounding off the top five D&O concerns is the risk of health and safety and environmental prosecutions. Environmental, social and governance (ESG) issues have moved up the boardroom agenda in recent years, with particular focus on health and safety and climate-related concerns (more on which, see the climate change article).

The risk of health and safety prosecutions has increased over the years and costs associated with such prosecutions can be considerable. Companies and directors are typically under a duty to do all that is “reasonably practicable” to protect the health and safety of their employees and also have duties to non-employees and must conduct their work activities in a manner that does not expose non-employees to health or safety risks.

The pandemic has created a myriad of exposures for directors and officers. Businesses and directors should remain alive to the possibility of investigation/prosecution in cases where there has been a serious failure to take appropriate protective measures, where substantial fines and imprisonment are available as sentencing options. There is also precedent for non-causative prosecutions, for example in cases where control measures have not been put in place, even where there may be causation issues over how those affected contracted the virus.



Commentary by Jon Vocking

With the shift to remote working models last year, cyber criminals have increasingly taken advantage of the vulnerabilities that continue to grow within a business’s digital infrastructure.

D&O underwriters are increasingly focusing on what necessary steps directors and officers have taken, and continue to take to protect their company’s digital assets and we are preparing our clients for this increased scrutiny. It is, of course, no surprise that we continue to see regulatory risk in the top 5. While ESG may be the subject of increasing focus, at the moment, we are not seeing many direct impacts on our clients’ renewals in terms of premium or policy exclusions.

Regional overview, Europe

Henning Schaloske, Clyde & Co

Europe

The past year once again saw businesses and society very much constrained and influenced by the pandemic. That said, the influence on D&O exposures has been fairly limited, including insolvencies, largely due to state moratoriums and financial aid given to distressed companies.

As we hopefully leave the pandemic behind and return to a new normal, the focus in D&O is very much on traditional exposures and emerging risks, and now of course the consequences of Russia/Ukraine conflict.

The latter has vast consequences for global economies and insurance, underlining why survey participants find the economic and geo-political climate are key factors for D&O risks. Amongst others, the Russia/Ukraine conflict will exert even further pressure on supply chains that already have been strained during the pandemic.

For directors and officers, in addition, there is comprehensive regulation incoming, including new supply chain due diligence requirements being implemented in Germany as part of a European Directive.

In particular, there is the potential for severe sanctions from this, from fines to new liabilities for companies. This is a key issue to watch in 2022 and beyond.

As we are emerging from the pandemic, two global systemic risks come to the spotlight even more, namely cyber risks and climate change.

The latter somewhat surprisingly has not made it into the top seven risks for Europe, but we anticipate it will get there soon, given the immense transition challenges, as well as increasing liability exposures, as exemplified by the Netherlands court judgment in 2021 against a large oil company.

Cyber again, dominates the risk hit list of European survey participants, and not surprisingly so, given the frequency and severity of cyber and ransomware attacks, the business interruption and costs in the wake of such, but also the exposure of companies and directors and officers in terms of more regulatory investigations, fines and liabilities.

Cyber and data privacy breaches will very likely be the field from which more and increased mass litigation is coming. Whether cyber and D&O insurance provides coverage for such liabilities is an area of the law that is prominently of concern to survey participants, and whether these fines are insurable at all remains a highly controversial and open question in many European jurisdictions. A related and equally controversial question is whether those companies fined may seek to recover the fine and other losses from the directors or officers.

While collective actions are steadily picking up across Europe, insured versus insured Side A claims remain dominant, together with regulatory exposures, which survey participants from Europe see as more concerning compared to other regions. This is for good reason, with criminal prosecutors long investigating individuals for corporate wrongdoing, and with more regulation incoming, including the implementation of the EU Whistleblower Protection Directive.

Not surprisingly, survey participants from Europe also show a great appetite for comparatively high D&O limits and for having or getting cyber insurance in place.

Risk ranking overview – by region

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)

Country of office	Europe
Cyber attack	71%
Data loss	65%
Cyber extortion	63%
Regulatory risk (including threat of fines and penalties)	46%
Shareholder actions/disputes	36%
Anti-trust law/regulation	34%
Risk of a health and safety/environmental prosecutions	46%
Return to work/COVID-safety/vaccination status	25%
Risk of employment claims	28%
Risks posed by supplier business practices	23%
Breach of human rights within your business operations	28%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	24%
Economic crime (your company/organisation as a victim)	38%
Bribery and corruption	42%
Risk of criminal penalties arising from breach of sanctions	37%
Social engineering crime (your organisation as a victim)	32%
Risk of other criminal proceedings	32%
Climate change	34%
Your company/organisation becoming a focus of a social media campaign	33%
Insolvency, bankruptcy or corporate collapse	33%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	27%
Pensions liabilities	19%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Regional overview, G.B.

Eve Richards, WTW

Great Britain

As a truly global survey across all continents and a broad spectrum of industries, company types and sizes, it is interesting to take a more in-depth look at how responses from Great Britain compared to those from other regions.

It's no real surprise cyber attack and data loss have maintained their respective first and second positions in the top five risks to directors and officers for the second year across all regions, including Great Britain.

This year's addition of cyber extortion to the top five list – at number three overall and number four for G.B. – indicates the level of concern the entire topic of cyber is posing to boards globally. There is little doubt this has been exacerbated by current geopolitical issues.

It is not only the impact of cyber attacks and extortion to the business operations to consider here, but also the potential for shareholder litigation following stock drops resulting from the reputational damage caused by such cyber incidences.

Data loss events too could transcend into D&O claims following losses suffered by the business from the associated fines and penalties. The trend for event-driven litigation means anything could result in a securities class action.

Boards are responsible for ensuring robust and resilient business platforms and the robustness of companies' IT systems has been severely tested in the context of global lockdowns. This pattern will undoubtedly continue as we remain in a period of potentially ever-increasing exposure to cyber risks in light of the Russia/Ukraine conflict.

This all comes at a time when capacity and the cost of insurance in the cyber market is extremely challenging. Could we potentially see the return of failure to maintain adequate insurance type claims around cyber exposure?

It is interesting to note G.B. survey respondents ranked these three risks proportionally less significant than all other regions by quite a margin. Meanwhile, regulatory risk, including threat of fines and penalties and risk of health and safety/environmental prosecutions, was almost equivalent to data loss and cyber extortion in the level of concern it poses to G.B. respondents. In fact, cyber extortion only comes fourth for G.B., being displaced by risk of health and safety/environmental prosecutions.

Post-pandemic, there is a risk that we will see an increase in activity from regulators whose activities have been constrained during lockdown. This could result in a significant uptick in costs on already struggling businesses as they try to find their feet post-pandemic.

COVID has surely played a part in driving concerns around health and safety. The obvious exposures for directors and officers are, of course, the potential for allegations of corporate manslaughter or occupational health breaches resulting from a failure to ensure adequate health and safety in the workplace.

Looking forward to 2022, ESG is a hot topic on boardroom agendas, as well as the media's. ESG is also becoming an increasing area of focus in the insurance market. It is clear any disclosure requirements may create liabilities, but how companies and boards tackle the issue of complying with their ESG requirements will be as big a liability as not complying or reaching targets.

Boards will need to fully understand all of this before acting, or could bear the brunt of claims arising from the mishandling of their ESG polices.

As directors continue to grapple with so many of the age-old risks driving litigation, there is also a wave of emerging and rapidly evolving risks to carefully consider, particularly given the wider impact of their actions on the environment and society as a whole.

One small consolation here is that after the last two extremely challenging years in the D&O insurance market, there is some relief in conditions afoot to help protect them from many of these risks.

Risk ranking overview – by region

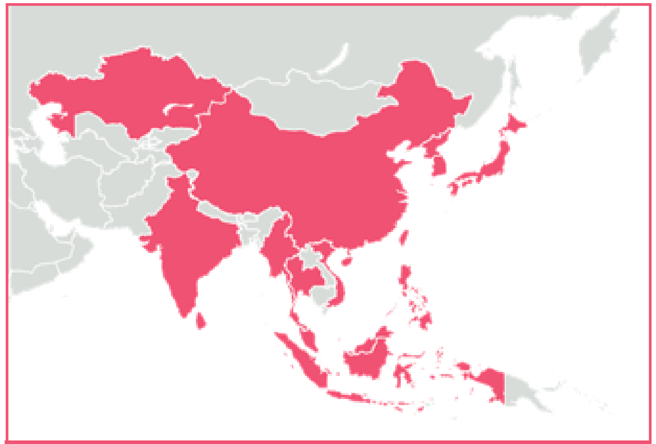
How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)

Country of office	G.B.
Cyber attack	47%
Data loss	43%
Cyber extortion	36%
Regulatory risk (including threat of fines and penalties)	35%
Shareholder actions/disputes	11%
Anti-trust law/regulation	10%
Risk of a health and safety / environmental prosecutions	40%
Return to work/COVID-safety/vaccination status	11%
Risk of employment claims	14%
Risks posed by supplier business practices	13%
Breach of human rights within your business operations	8%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	8%
Economic crime (your company/organisation as a victim)	13%
Bribery and corruption	13%
Risk of criminal penalties arising from breach of sanctions	15%
Social engineering crime (your organisation as a victim)	14%
Risk of other criminal proceedings	10%
Climate change	24%
Your company/organisation becoming a focus of a social media campaign	22%
Insolvency, bankruptcy or corporate collapse	10%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	10%
Pensions liabilities	11%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Regional overview, Asia

Namit Mahajan, WTW



Directors' and officers' risk landscape has witnessed rapid evolution in Asia in recent times. While the universal trends such as the impact of pandemic, environmental and other ESG issues and growing concerns around cyber claims dominated this transition, closer to home, a spate of changes to the regulatory environment acted as a key catalyst. Some of the key trends witnessed in Asia include the following:

China: Effective 1 March 2020, the revisions to Securities Law of People's Republic of China (PRC) came into effect. These revisions further improved the basic system, embodying the direction of marketisation, rule of law, and internationalization. Amongst the various highlights are the key revisions around improving the investor protection system, significantly increasing the cost of securities violations and further strengthening of information disclosure requirements.

These changes increase the uncertainties around potential risks for directors and officers considerably. There has been a recent ruling which marks the first ever securities class action ruling in China and is expected to have a long-lasting effect on D&O litigation trends in the country. Despite these developments, it is notable that the risk of shareholder actions/disputes was not highly ranked by respondents in Asia, with only 51% of respondents considering that the risk was very significant or extremely significant.

51%

of respondents consider that the risk is very significant or extremely significant

Japan: The Companies Act Reform Bill, which came into force on 1 March 2021, represents a key step towards enhanced corporate governance standards in Japan. Additionally, the recent revisions to the Corporate Governance Code of the Tokyo Stock Exchange further stipulated fundamental principles for effective corporate governance for listed entities. These key changes include provisions around the mandatory appointment of outside directors for listed companies and establishment of systems for appropriate determination of remuneration for directors and the like. Most importantly, the Reform bill for the first time established the procedure for conclusion of D&O Liability insurance policies, involving approval of a shareholders' meeting or, for a company with a board of directors, approval of the board of directors.

It further established rules under which companies may indemnify their directors and officers against expenses incurred in defending an action involving their liability. With developments such as these, it is unsurprising to see that regulatory risk is identified as the number three risk in Asia, with 64% of respondents identifying it as very significant or extremely significant.

Pandemic: The focus has now shifted from the immediate impact of the pandemic to long-term issues, especially in emerging economies in Asia. The uncertainties around recovery, operational adjustments to the ever-changing regulatory and compliance landscape, and the mismanagement of disclosures have added to the long list of unanticipated risks for directors and officers. We expect continued and detailed scrutiny on financial sustainability, work force management and future business prospects as the part of the lingering impact of the pandemic on the D&O Liability landscape.

U.S. class action exposure for American Depository Receipts ("ADRs") - listed companies – The growing extra-territorial risk of U.S. securities litigation through ADRs has been an emerging concern for listed companies in Asia with either sponsored or unsponsored ADRs. U.S. plaintiff firms continue to target international companies through their ADRs and there has been a significant uptick in such attempts in recent times. The financial impact of litigating in the U.S. could be severe, hence why we are witnessing heightened concerns around this risk from a D&O liability perspective. However, recent developments in the U.S. courts may ameliorate some of this concern for companies with unsponsored ADRs.

Risk ranking overview – by region

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)

Country of office	Asia
Cyber attack	70%
Data loss	70%
Cyber extortion	63%
Regulatory risk (including threat of fines and penalties)	64%
Shareholder actions/disputes	51%
Anti-trust law/regulation	42%
Risk of a health and safety / environmental prosecutions	48%
Return to work/COVID-safety/vaccination status	51%
Risk of employment claims	50%
Risks posed by supplier business practices	61%
Breach of human rights within your business operations	52%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	53%
Economic crime (your company/organisation as a victim)	49%
Bribery and corruption	56%
Risk of criminal penalties arising from breach of sanctions	51%
Social engineering crime (your organisation as a victim)	48%
Risk of other criminal proceedings	44%
Climate change	58%
Your company/organisation becoming a focus of a social media campaign	46%
Insolvency, bankruptcy or corporate collapse	42%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	45%
Pensions liabilities	24%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Regional overview, North America

Lawrence Fine, WTW

North America

The fact that cyber attack was rated in North America as the number one risk, as it was in four other geographic regions, not including Latin America, is not surprising. It's worth noting the next two ranked risks are also related to cyber, with cyber extortion in third position and data loss in second place and the two being closely related to each other since extortion creates an increased risk of data loss.

While North America has seen many headlines relating to cyber risks, particularly cyber extortion, it is still debatable whether in dollars and cents cyber-related risks for directors and officers deserve all three of the first three spots on the risk survey.

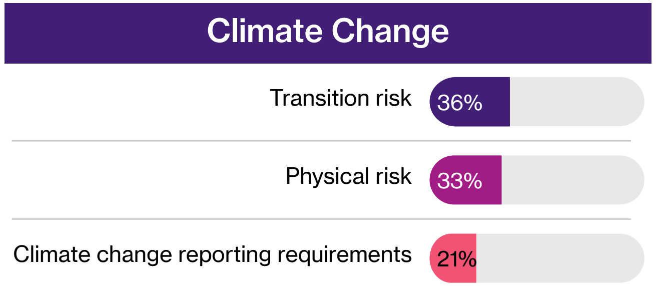
North America is the only region where the directors and officers rated 'return to work/COVID safety' and 'social engineering crime' as numbers four and five respectively. These two categories did not appear in any other region's top seven list. In the U.S. in particular, there has been more COVID-related litigation than in other regions, although perhaps not as much as many insurers may have anticipated. A rise in social engineering crime in the last few years has resulted in actions by some insurers to exclude such risks.

'Supplier business practices' came in as the sixth-ranked risk, compared to its fifth-place rating in Asia. (This was not a major factor anywhere else). It seems North American respondents may have anticipated the current global supply chain issues and the ripple effect these could create for indirectly effected companies.

The appearance of regulatory risk at the bottom of the top-seven ranked risks is surprising, given that 2021 saw record SEC whistleblowing activity and newly aggressive positions being announced by both the U.S. Department of Justice and Securities Exchange Commission (see separate article on regulatory risk in the U.S.).

It also seems surprising shareholder class actions did not make the top list, with only 18% ranking it as "very significant" or "extremely significant". This may be partly because of the recent drops in class action filing volume, although it did not rank highly as a risk last year either.

Just 18% of directors and officers rated climate change as "very significant" or "extremely significant" (lower than every other region). In a series of specific sub-questions relating to climate change, transition risk was rated at 36%, physical risk at 33% and climate change reporting requirements at just 21%. This is compared to percentages ranging between 41% in Great Britain to 73% in Asia. This is likely to change in reaction to anticipated further legal requirements concerning climate change disclosures being imposed by the SEC.



% of NA respondents who considered that each of these categories of climate change risk to directors were "Very significant" or "Extremely significant". Note: only respondents who considered that climate change was at least "significant" were asked this question.

On the insurance coverage side, North America stands alone in rating choice of lawyer as the number one issue, even above the category of 'how claims against directors and officers will be controlled and settled'. Not appearing in the North American top seven coverage concerns is 'cost of legal advice at the early stages of an investigation' which featured in all other regions' top seven rankings. This suggests directors and officers in North America are more satisfied than their counterparts around the world in terms of protections for insured persons in the early stages, perhaps because of the proliferation of early triggering features such as informal inquiry and interview coverages.

Commentary by Elizabeth Adamson, WTW

What is clearly coming through from the survey results is the increasingly complex environment that Canadian companies are experiencing and having to navigate. Directors and officers, as well as underwriters, need to make decisions based on the challenge of actual, current and theoretical risks. Add on evolving technology, increasingly savvy bad actors doing their best to exploit weaknesses, regulators trying to keep abreast of rapid changes, and emerging industries that do not yet have a track record of exposures driving claims (such as electric vehicles, carbon capture, digital currencies) and we only begin to appreciate how hard it is to navigate the economy successfully and mitigate claims.

The top seven risks by region for North America falling into broader categories of cyber, regulatory, and health and safety, reflect the transitional economy as we emerge from pandemic lockdowns while anticipating the next global risks. The most important D&O insurance coverage issues reflect directors and officers needing resources and additional expertise to augment their decision making: choice of lawyer/counsel; whether there is cover for legal advice at the early stages of an investigation; whether there is coverage to appoint a public relations expert. These important coverage issues identified are also reflective of the changes to D&O liability terms and conditions we are seeing in Canada as insurers try to balance covering these risks while being sustainable for Insureds and managing inflationary costs.

Risk ranking overview – by region

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)?

Country of office	North America
Cyber attack	64%
Data loss	62%
Cyber extortion	54%
Regulatory risk (including threat of fines and penalties)	31%
Shareholder actions/disputes	18%
Anti-trust law/regulation	18%
Risk of a health and safety / environmental prosecutions	15%
Return to work/COVID-safety/vaccination status	38%
Risk of employment claims	31%
Risks posed by supplier business practices	33%
Breach of human rights within your business operations	10%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	13%
Economic crime (your company/organisation as a victim)	23%
Bribery and corruption	10%
Risk of criminal penalties arising from breach of sanctions	18%
Social engineering crime (your organisation as a victim)	36%
Risk of other criminal proceedings	10%
Climate change	18%
Your company/organisation becoming a focus of a social media campaign	24%
Insolvency, bankruptcy or corporate collapse	3%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	3%
Pensions liabilities	13%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Regional overview, Latin America

Marcela Visbal Acuña, WTW

Latin America

The risk concerns of global companies and their directors are unique to their circumstances, and a director in Latin America is very likely to have different priorities from a director in Asia or Europe for example. That said, the risk concerns are often similar in nature and it is the degree of intensity which is the variable factor.

No risk overview can ignore the volatility of global events. The pandemic and more recent geopolitical events have changed the global risk perspective beyond all recognition.

In the Directors' Liability Survey, the risks for the business that most concerned directors are the economic climate and cyber-attacks, followed by the consequences of the pandemic, and then technological advances and climate change. These results correlate with the report on risks published by the World Economic Forum last year and we can say that Boards are focusing on the same risks globally.

Focusing specifically on Latin America, we see that as a region it places the most importance on economic climate as an underlying risk. In second place are the consequences of the COVID-19 pandemic with cyber attacks in third place. The region also attaches greater importance to all risks in general than in the other territories.

In Latin America, the lack of regulations on significant issues such as climate and legal and political uncertainty, predominate and, therefore, the consequences of the pandemic are different from those that other regions may face. This is reflected in the region-specific results of the survey. These aspects also affect the development of D&O insurance in Latin American countries, in which the hardening of the market affected it more than in other locations. There was a decrease in capacity due to the lack of interest of the markets in providing support as a result of additional risks to those faced in other countries and high volatility.

Directors' concerns on climate change are perhaps understandable, given the lack of regulation which has historically left a significant impact in Latin America and may result in increasing the risk in the future.

Regarding technology and cyber risks, there is also a lack of regulation and awareness of the need for more robust security and controls. Companies in Latin America are finally beginning to worry about the development of controls and security, having previously considered themselves outside the major events that exist at a global level. The truth is that in any case it is a region impacted by cyber-attacks where there is no adequate prevention or management of events, nor, in most cases, a transfer of risk.

In summary, it is possible that the lack of regulation and management of key risks together with limited ways to transfer risks are likely contributory factors in making the concerns of Latin American respondents more pronounced across many of the risks.

Risk ranking overview – by region

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)

Country of office	LatAm
Cyber attack	77%
Data loss	86%
Cyber extortion	80%
Regulatory risk (including threat of fines and penalties)	75%
Shareholder actions/disputes	73%
Anti-trust law/regulation	38%
Risk of a health and safety / environmental prosecutions	67%
Return to work/COVID-safety/vaccination status	68%
Risk of employment claims	67%
Risks posed by supplier business practices	62%
Breach of human rights within your business operations	66%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	44%
Economic crime (your company/organisation as a victim)	75%
Bribery and corruption	74%
Risk of criminal penalties arising from breach of sanctions	69%
Social engineering crime (your organisation as a victim)	69%
Risk of other criminal proceedings	50%
Climate change	52%
Your company/organisation becoming a focus of a social media campaign	63%
Insolvency, bankruptcy or corporate collapse	67%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	42%
Pensions liabilities	42%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Regional overview, Australasia

Lucinda Lyons, Clyde & Co, Robert Weaver and Jill Stewart, WTW

Australasia

Lucinda Lyons - Clyde & Co

The 2022 survey provides a fascinating insight into the liability concerns of Australian directors and officers. The results speak to a market that appears comfortable managing traditional risks, such as employment claims, insolvency and regulatory risk, and more concerned with emerging, less well-understood risks such as cyber attacks, data loss and cyber extortion.

Most interesting is that the significance of shareholder actions/disputes is lower when compared to other regions. This is despite Australia being one of the most litigious countries for securities class actions. Directors' sentiment may reflect their belief that recent government law reform of securities law and litigation funding will have the desired effect.

It may also indicate directors have faced the risk of securities actions in record numbers over the last ten years and have adapted to the environment with robust risk management. We hope this presents an example to directors and officers grappling with the emerging cyber and data loss risks. These risks can be managed with appropriate risk mitigation once correctly understood.

The risk of health and safety and environmental prosecutions was the fourth-highest regional risk behind cyber and data loss risks. Australia continues to be a jurisdiction that takes the health and safety of workers seriously, and health and safety regulators are active in ensuring compliance.

The impact of government responses to COVID-19, including vaccine mandates and prolonged lockdowns in Australia, may account for the heightened assessment of this risk. Australian businesses have needed to pay particular attention to ensure the safety of their workers during the pandemic.

The emergence of climate change as an area of significance is likely to reflect Australia's emergence as the tip of the spear for the extreme physical manifestation of climate impact. It has become one of the most active jurisdictions for climate change litigation activists.

Jill Stewart and Robert Weaver, WTW

Securities Class Actions and Class Actions

AU: 2021 saw a reduction in new filings and increased enthusiasm by the Government and regulators to control litigation funding and increasing class action activity. We expect continued disruption into 2022, with funder returns potentially being capped under a proposed bill, potential changes to the class action regulatory attitude following the Australian general election in mid-2022, and an early win in 2022 for a securities claim defendant. However, the confidence this win might have given corporates and their insurers has been muffled by the remission of another securities class action back for hearing on liability issues, and the first potential securities class action damages award following a Court of Appeal decision.

NZ: At present, New Zealand does not have a statutory class actions regime. Based on feedback received in response to two issues papers on litigation funding and class actions released in 2020 and 2021, Te Aka Mautua o te Ture Law Commission considers that New Zealand should introduce a statutory regime. The Commission is due to provide its final report in May 2022 and is expected to directly address the tension between the benefits of class actions and litigation funders and their impact upon the business environment in New Zealand. The report is also expected to bring clarity to procedural controversies such as the status of opt-out orders (the Supreme Court has unanimously allowed an opt-out class action to proceed for the first time, despite the lack of a specific statutory regime).

Side A and B claims

AU: In late February 2022, the High Court of Australia handed down a ruling that shareholders of a company in liquidation can use the public examination powers in Part 5.9 the Corporations Act 2001 (Cth) to investigate personal claims against the company's former directors and its auditor, even though those personal claims will not benefit the company or its creditors. Such examinations had previously been undertaken exclusively by liquidators and regulators. The High Court's decision opens up the public examination process to parties who may have a potential claim against the former directors and advisors of a company in liquidation.

Directors, D&O insurers, and professional indemnity insurers can now expect an increase in the use of public examinations by shareholders, and litigation funders, to investigate potential securities class actions against directors and advisors.

Regional overview, Australasia

Lucinda Lyons, Clyde & Co, Robert Weaver and Jill Stewart, WTW

Defence costs

NZ: The Government is considering a new third-party claims regime that could repeal s.9 of the Law Reform Act 1936 (N.Z.). These reforms propose to place insurers in the shoes of the insured party during proceedings brought by a claimant against the policyholder. If this goes through, it will impose greater obligations on the insurer and insured with respect to claims made by an injured third party, and will challenge the need for separate defence cost limits.

Climate change/ESG

AU: Australia continues to be a market where activist-based litigation is a common feature, with environmental groups targeting ASX-listed company and carbon heavy companies with actions around misleading conduct, market disclosures and greenwashing (for example, *Australasian Centre for Corporate Responsibility v Santos Limited*, where an environmental advocacy group has alleged certain 'green' claims made by Santos are misleading and deceptive in breach of the Corporations Act 2001 (Cth)). Despite a setback with another case in March, where a novel duty of care to prevent intergenerational harm through climate change was successfully appealed, Australia is becoming the jurisdiction of choice for creative climate litigation.

NZ: N.Z. has passed the world first climate reporting legislation under the Financial Sector (Climate-related Disclosures and Other Matters) Amendment Act 2021. Climate-related disclosures are now mandatory for some organisations in N.Z., including large publicly listed companies and insurers.

These obligations will apply to around 200 entities, including all licensed insurers with greater than $1b in assets or annual premium income over $250m. Reporting will be against a standard that will be developed with reference to the governance, strategy, risk management, and targets of the relevant organisations.

Regulatory

AU: Australian Securities and Investments Commission (ASIC) key priorities for 2022 include the management of cyber risks, specifically around compliance with breach-reporting obligations, continuous disclosure obligations and regulatory action for breach of AFS license. Other priorities include climate change governance practices, and egregious governance failures or misconduct resulting in corporate collapse which are relevant in terms of insolvency trends detailed below. In relation to cyber security compliance, ASIC is positioned to take an 'active and targeted approached to enforcement', impacting AFSL holders and their authorised representatives.

A recent focus for clients has been understanding ASIC's views on AFSL requirements and wider gatekeeper and director-related obligations. ASIC analyses cybersecurity through the lens of whether an organisation has adequate risk management systems and adequate resources, such as technology resources whilst AFSL holders are also required under the Corporations Act 2001 (Cth) to comply with a range of obligations, including those in sections 912A and 912B. 2022 will also see the introduction of the new Financial Accountability Regime (FAR), which extends and replaces the Banking Executive Accountability Regime (BEAR).

At a high level, FAR will impose obligations on certain 'accountable persons' to ensure reasonable steps are taken to prevent material contraventions of financial services laws – it expressly recognises persons may be subject to civil penalties if they are found to have accessorial or ancillary liability to a contravention of the regime. Under the FAR, there is no prohibition on indemnification or insurance for accountable persons, noting there was a stringent prohibition for this under the previous regime (BEAR).

FAR will apply to banks and other ADIs from 1 July 2022, and to general insurers, life insurers, private health insurers and superannuation trustees from 1 July 2023. Continued tighter regulation of big tech - Australian regulators including the ACCC and the Australian Information Commissioner have joined forces to form the Digital Platform Regulators Forum, as pressure to rein in the tech giants builds globally. ACCC is to focus on supply chain competition, COVID-related disruptions and the protection of consumers, particularly relating to manipulative or deceptive advertising and marketing practices in the digital economy.

AUSTRAC has a continued focus on casinos and systemic non-compliance with anti-money laundering and counter terrorism financing laws. AUSTRAC recently commenced proceedings against two casinos owned by Crown Resorts. Interestingly, only the entities have been named as respondents, not any directors or officers. We expect increased regulation for fintechs, including BNPL and crypto exchanges and also an increased focus on consumer protections.

NZ: The FMA outlined its priorities in March, with a focus on revisions to the FMA's Conduct Guide to reflect legislative principles enabling the FMA's regulation of banks and insurers. The FMA also indicated priorities in monitoring climate-related disclosures and cyber resilience.

The FMA plans to release draft standards for consultation in relation to N.Z.'s new mandatory climate reporting regime and release an information sheet outlining the FMA's expectations of organisations in formulating their cyber security plans.

Regional overview, Australasia

Lucinda Lyons, Clyde & Co, Robert Weaver and Jill Stewart, WTW

The New Zealand Court of Appeal has issued a 2021 decision not to impose a new tort of breach of duty to stop damage to the climate system. This could trigger tougher statutory liabilities on companies and their boards by regulators. The Court found climate change calls for a sophisticated regulatory response at a national level, supported by international co-ordination.

The Minister of Commerce and Consumer Affairs has provided their annual letter of expectations to the N.Z. Commerce Commission requesting action on new legislative instruments with respect to the enforcement of consumer credit, the fuel industry, cartel conduct regimes, and the contestability of dairy markets.

Insolvency

AU and NZ: Increasing risk in 2022 as government support is withdrawn and both the ATO and IRD recommence collections. Key industries at risk – construction, hospitality, and retail. Australia's construction industry has already seen one major company go insolvent this year, with more forecast to follow.

Challenges ahead include a shortage of employees, global supply chain issues and increasing interest rates.

Risk ranking overview – by region

How significant are the following risks for the directors and officers of your organisation (whether financially or reputationally)?

Country of office	Australasia
Cyber attack	57%
Data loss	46%
Cyber extortion	46%
Regulatory risk (including threat of fines and penalties)	32%
Shareholder actions/disputes	6%
Anti-trust law/regulation	12%
Risk of a health and safety / environmental prosecutions	41%
Return to work/COVID-safety/vaccination status	20%
Risk of employment claims	14%
Risks posed by supplier business practices	11%
Breach of human rights within your business operations	11%
Board/ management/ company takeover or other forms of activism by shareholders or institutional investors	6%
Economic crime (your company/organisation as a victim)	26%
Bribery and corruption	9%
Risk of criminal penalties arising from breach of sanctions	21%
Social engineering crime (your organisation as a victim)	17%
Risk of other criminal proceedings	6%
Climate change	31%
Your company/organisation becoming a focus of a social media campaign	22%
Insolvency, bankruptcy or corporate collapse	8%
Risk of proceedings in a jurisdiction outside your organisation's main home jurisdiction	9%
Pensions liabilities	3%

(% of 'Very significant' or 'Extremely significant')
Source: Directors' Liability Survey 2022

Class actions

Edward Kirk, Clyde & Co

Despite the fact that the survey respondents in the U.S. did not rank the risk of shareholder actions highly, this risk remains of high concern to insurers.

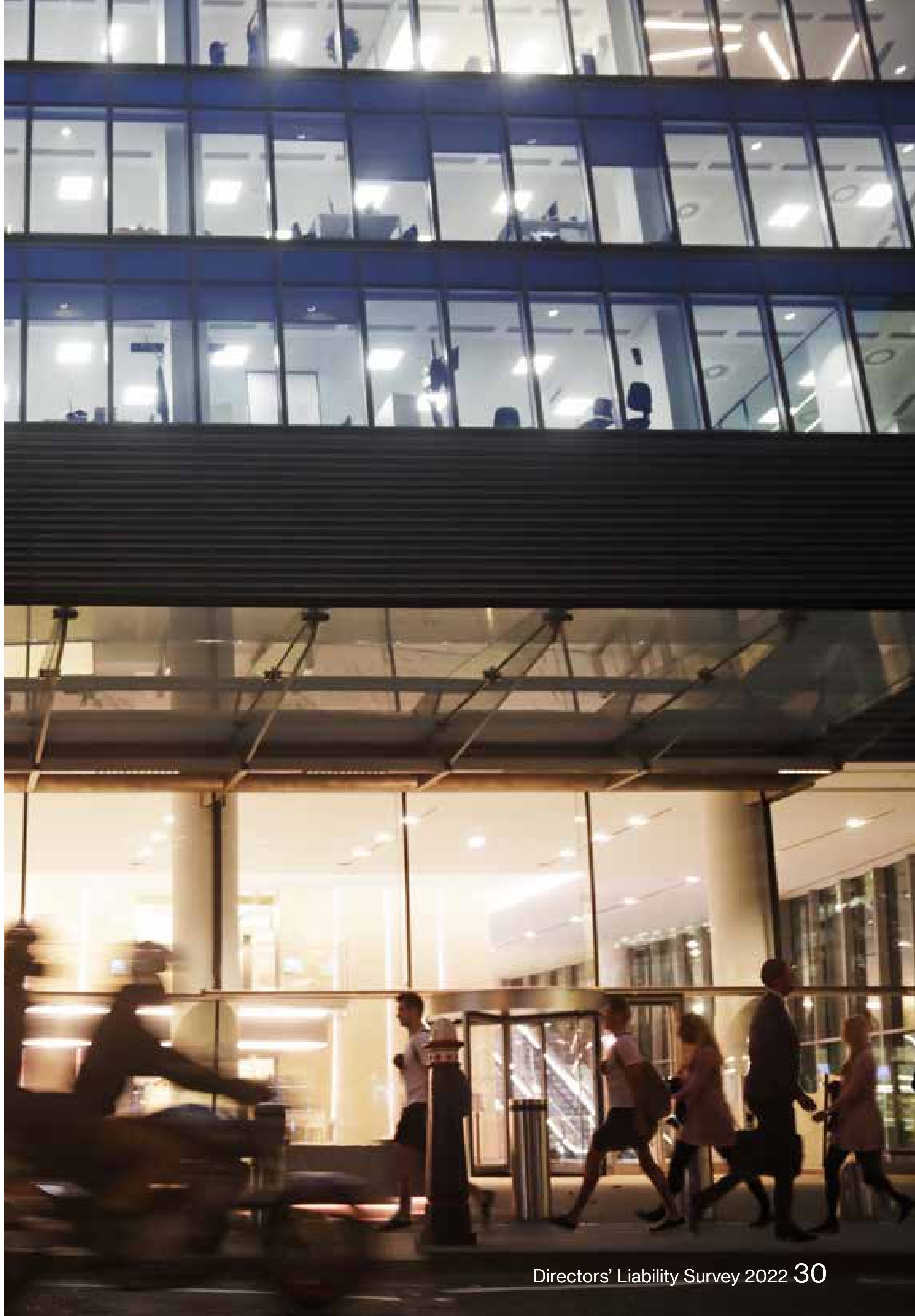
In the U.S., there were a number of favourable developments for defendants in 2021, resulting in a substantial decrease in the number of U.S. securities class actions, but a number of other trends could reverse these gains in 2022.

According to Cornerstone Research's Securities Class Action Filings 2021 Year in Review, in 2021, the number of new U.S. securities class action filings declined by 35% from the prior year, or from 333 in 2020 to 218 in 2021. The 218 new cases in 2021 represents the lowest number since 2015, and almost half of the number of new filings in each year during the 2017-2019 period when more than 400 new cases were filed each year.

The spike in new filings during the 2017-2020 period was largely due to the dramatic increase in cases relating to mergers and acquisitions (M&A) that were often settled much quicker and more cheaply than core, or more traditional, filings. More than 100 M&A securities class actions were filed each year during the 2017- 2020 period, but the number of new M&A class action filings dropped to just 18 in 2021, or by 82% compared to 2020. Core filings fell by a more modest, but still significant 17%. The main reason for the drop in M&A class action filings may be a noted increase in merger objection suits being brought by individual plaintiffs; settlements of such suits do not require judicial approval or class notice and so are difficult to track.

The filing rate, or percentage chance a publicly listed company will be sued in a U.S. securities class action, dropped to 4.2% in 2021, compared to 6.3% in 2020 and over 8% in the period 2017-2019.

Plaintiffs continued to target companies domiciled outside the U.S. during 2021, but at a lower rate than in prior years. Plaintiffs filed a total of 42 securities class actions against non-U.S. issuers in 2021, compared to 88 in 2020. In 2021, only 19 new cases were brought against Asian companies, compared to 31 cases in 2020. Of the 19 filings against Asian companies, 18 were brought against Chinese companies. Shareholders filed 13 securities class actions against European companies in 2021, and five of those cases named healthcare or pharmaceutical companies. Seven cases were filed against Canadian companies. The litigation rate for non-U.S. companies dropped to 3.5% from over 9% in 2018.



Class actions

Edward Kirk, Clyde & Co

Following the U.S. Supreme Court's 2018 ruling in Cyan, which found state courts have concurrent jurisdiction with federal courts under the Securities Act of 1933 ('the 33 Act'), plaintiffs filed a high number of cases relating to securities offerings in state courts, particularly in California and New York. Plaintiffs filed 35 state court securities class actions in 2018 and 52 in 2019.

These state court cases increased potential exposure to defendants, who often were forced to defend parallel cases in both federal and state courts. State courts often provide a more favourable forum for plaintiffs, and cases in state courts are often more difficult to dismiss than federal cases. In 2020, however, the Delaware Supreme Court in Sciabacucchi upheld corporate charter provisions requiring shareholders to bring '33 Act claims in federal courts. As a result, new filings in state courts fell to 23 in 2020 and 13 in 2021 and will likely continue to fall as more corporations adopt federal forum selection provisions.

New filings in state courts

2020	2021
23	13

Cases relating to special purpose acquisition companies (SPACs) are a significant trend that may result in higher numbers of securities class actions in 2022. In 2020 – 2021, SPAC initial public offerings (IPOs) increased dramatically from 59 in 2019 to 248 in 2020 and 613 in 2021 for total proceeds of almost $250 billion in that two-year period. These complex and high value transactions caught the attention of the plaintiffs' bar, which filed five SPAC securities class actions in 2020 and 32 in 2021.

As of December 31, 2021, there were over 575 SPACs seeking merger targets, and it is expected more securities class actions involving SPACs will be filed in 2022 as SPACs compete for fewer acquisition targets.

Another trend in 2021 was new filings relating to COVID-19. There were 17 COVID-19 securities class actions filed each year in 2020 and 2021. Many of these actions related to misrepresentations relating to temporary increases in business, outbreaks in facilities, or other disruptions from the pandemic. These cases are expected to decrease as the pandemic winds down, but at the end 2021, a number of securities class actions were filed against companies, such as Peloton, whose business prospered early in the pandemic but fell off in recent months.

Cyber-related securities class actions have not yet had a major impact on the number of new filings or settlements but could have a significant impact on securities class action trends in the near future. In 2021, six cybersecurity class actions were filed, compared to four in 2020 and three in 2019. The number of cyber cases may increase significantly in coming years as investors and regulators increasingly focus on cybersecurity disclosures.

Cybersecurity class actions filed

2021	2020	2019
6	4	3

There has been an increase in securities class actions filed by investors in cryptocurrencies. In 2021, 11 of these actions were filed, compared to 12 in 2020, 4 in 2019 and 14 in 2018. These cases often allege the defendants offered or sold unregistered securities in violation of securities laws, and liability will depend on the particular type of cryptocurrency at issue.

Other areas worth watching include ESG and climate change-related disclosure shareholder litigation, in which investors and regulators have shown increasing interest. Notably, the Chairman of the SEC, Gary Gensler, has made climate disclosure a focus of his regulatory agenda, resulting in the recent issuance of a proposed sweeping climate disclosure rule.

Regional views by Clyde & Co

UAE - Mark Beswetherick

Class action regimes are still not widespread in this region, even in the common law financial centres of the DIFC and ADGM. However, Saudi Arabia introduced a new class action regime in 2017 for listed Saudi companies. Already, this has led to one class action involving Mohammed Al Mojil Group, a construction company in which a high value damages claim was upheld against the former directors. Two further class actions are pending against the former D&Os of a Saudi Arabian telecoms company and, very recently, against the D&Os and some employees of an Insurance Company. The second class action followed the lawsuit filed by the Capital Market Authority (CMA) against the board of directors and the audit and executive committees in which they were convicted and fined SAR 1.3 million. This demonstrates the willingness of Saudi investors to pursue class action litigation for losses suffered as a result of regulatory and accounting failures.

Class actions

Edward Kirk, Clyde & Co

Europe - Henning Schaloske

Collective redress continues to be on the rise across Europe and is increasingly becoming a major risk driver. Next to shareholder actions, participants in the survey identify cyber as a headline risk in Europe. In particular, there is a lot of activity in the legislative field, with the pending adoption of the European Directive (EU) 2020/1828 on representative actions into domestic laws, as well as LegalTech and litigation funders implementing mass litigation options in the existing procedural framework, aiming at enforcing claims against companies in breach of the General Data Protection Regulation (GDPR).

Australia – Patrick Boardman

There have been several important recent developments in the Australian class action space, some of which will only come to a head in 2022:

- There have been legislative changes to Australian continuous disclosure laws and associated misleading deceptive provisions of the Corporations Act 2001, said to be brought in to prevent opportunistic class actions by bringing a fault-based system akin to that in the U.S. and U.K., rather than the effective strict liability of the current system. There is now a requirement of knowledge, recklessness or negligence in respect of a company's failure to determine price sensitive information disclosure. Our view is little will change with these amendments.
- There is ongoing governmental control of the burgeoning litigation funding business, with latest proposals for a requirement members must receive at least 70% of any return. While this could reduce the quantum of larger class actions, it could make smaller class actions harder to settle. There is also greater court scrutiny of both lawyer and funder returns.
- There has been legislative change in the State of Victoria which is now the only Australian jurisdiction allowing lawyer contingency fees for class actions. Since this change, all Australian shareholder class actions have been filed in this jurisdiction.
- There is still ongoing uncertainty about some important class action procedural rules, principally in regard to class closure, which make the assessment and settlement of class actions very difficult if the size of the class is not known.

For more than 20 years, no shareholder class actions went to judgment. Recently, however, there have been three shareholder class action judgments. The respective results of those judgments have been the following: the defendant company lost on liability but won on loss and causation; the defendant company won on liability at first instance which has just been overturned on appeal; and the defendant company won on liability and the judgment will not be appealed. In addition to providing long-awaited judicial guidance, the decisions set out what is required for a successful defence of a shareholder class action.

Asia/Hong Kong - Simon McConnell

Asia is broadly less litigious than the U.S. or Australia, and the class action regimes largely mirror this reality. Although relatively benign, this is not to say exposures are low or non-existent and there are developments regionally creating real underwriting risk for D&O and IPO underwriters.

Mainland China's relatively new 'class action' (representative litigation) system with Chinese characteristics includes both opt in and opt out variants, together with strong regulator involvement.

In December 2021, the first Chinese securities action ruling awarded damages of USD 385 million against the listed entity and its management. Similar investor actions with regulator support continue in Taiwan and other Asian jurisdictions.

In Hong Kong, the companies and securities regulator (SFC) has the power to seek redress for shareholders, which it does do in the very substantial cases. This power may become more relevant as the Chinese and U.S. capital markets continue to decouple, with U.S.-listed Chinese companies expected to continue so-called 'homecoming' direct and secondary listings in Hong Kong, with the former giving access to mainland capital via the Stock Connect regime.

South Africa - Daniel Le Roux

South Africa is seeing a steady uptick in the use of class action litigation to pursue claims against companies, notably in group injury and compensation claims relating to cartel behaviour, silicosis (occupational lung disease) and listeriosis (food contamination).

The development of a procedural framework for class actions in South Africa has encouraged a more organised plaintiffs' bar which is finding support from litigation funders and established plaintiff law firms in other jurisdictions, such as the U.S. and Australia.

It has become common in class action suits in South Africa to require litigation funders put up security for costs at class certification stage. It is also advisable for defendants' attorneys to require plaintiffs' attorneys to disclose their contingency fee agreements upfront to ensure compliance with the Contingency Fees Act. We anticipate claims involving D&Os who may be joined as defendants or third parties to class action proceedings.

Cyber attack, data loss, cyber extortion

John Moran and Marc Voses, Clyde & Co

A robust 67% of respondents worldwide believe risks to their organisation's business operations presented by cyber attacks are second only to those created by the economic climate. Respondents in Europe rank cyber attack risks solidly in first place, while it is tied for first with economic climate by North American respondents, with Australasian respondents ranking the risk second behind COVID-19 and lockdown measures.

With the daily barrage of media reports on high-profile cyber events, it is unsurprising the three categories of cyber risk put to respondents account for the top three risks: with the first being cyberattacks, second, data loss and third, cyber extortion.

With this backdrop, global regulators continue to urge directors to step up and ensure cyberrisk is well examined and addressed by their businesses, from safeguarding data 'crown jewels', to implementing good cyber hygiene and ensuring management are primed and ready to respond to and recover from a cyber attack.

2021 was a wakeup call for businesses operating in core critical infrastructure sectors in particular, as governments, including China, Australia and the U.S., joined the E.U. in implementing regulatory regimes to protect core critical infrastructure assets from cyber attacks. Existing regulatory regimes are also being enforced with more regularity that are oftentimes accompanied by statutory fines and penalties for non-compliance.

A global risk unconstrained by borders

Whilst the perception of this risk differs from region to region, this year's results clearly point towards an intensifying concern of cyber attacks and data risk across the globe. Off the back of the Colonial Pipeline, JBS and Microsoft Exchange attacks, North American respondents reported a significant shift in concern about the risks of cyber incidents for directors: 64% of respondents in 2022 perceived the risk of cyber attacks as 'very significant' or 'extremely significant', as opposed to 52% in 2021.

Cyber attack, data loss, cyber extortion

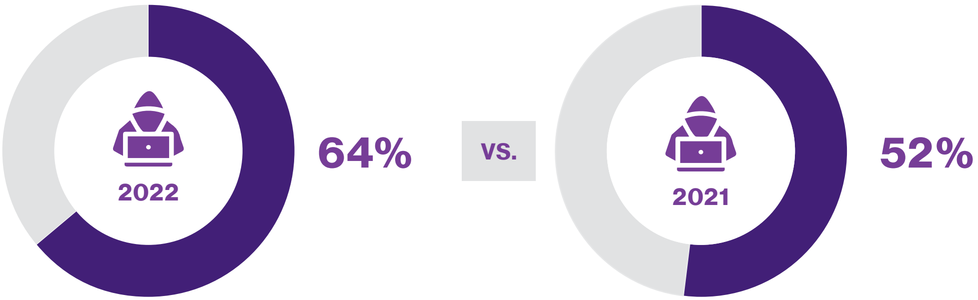
John Moran and Marc Voses, Clyde & Co

Even higher figures were reported in Europe and Asia, however just 57% of Australasian boards judged the risk of cyber attacks as either very or extremely significant, which may be explained by the less mature regulatory environment and the less frequent targeting of companies in the region.

Future predictions

It is likely regulators will continue to assert more power in developing regimes. In Australia for example, the Office of the Australian Information Commissioner has increased activity over the last 12 months, a trend likely to continue in light of the recent litigation and may set the groundwork to commence the class action landscape for breach of privacy claims within Australia.

North American respondents reported a significant shift in concern about cyber incidents:



Perceived the risk of cyber -attacks as 'very significant' or 'extremely significant'

Evolving landscape of risk

The changing risk landscape is likely to increase concerns about cyberrisk, especially in uncertain geopolitical times. We have already seen an increased recognition of this risk, with 65% of respondents globally now recognising the threat of cyber attack as 'very' or' extremely significant', compared with 56% last year.

The threat of ransomware, for example, has become more sophisticated and this is explored more in the article: Cyber Extortion - ransomware and payment of ransoms.

In North America, state governments are increasingly enacting data privacy laws that require organizations to take control of their data and inform the public what data they collect and how they use it. Regulators, including those overseeing public companies and financial institutions, are becoming more active in pursuing those entities that suffer data breaches as a result of a failure to implement or adhere to a cybersecurity program.

We predict a continued uptick in regulatory enforcement actions, along with significant monetary fines for those organizations that suffer a cyber attack because of a failure to maintain an adequate cybersecurity program.

From the standpoint of cyberinsurance, we predict stricter underwriting requirements and increasing premiums could result in businesses being underinsured or uninsured.

In some respects, the visibility of the risks presented by cyber attacks and increased regulation have resulted in businesses improving their cybersecurity programs and addressing data collection practices.

We believe the entry of additional cyberinsurance capacity, coupled with assessing and monitoring an organizations' cybersecurity, will help reduce cyber attacks on those organizations using these products and services.

Regional views by Clyde & Co

South Africa – Daniel Le Roux

South Africa's long-anticipated data protection laws became effective in 2021, but regulatory oversight and enforcement is lagging behind.

The growing nature of this risk is in part due to limited policing expertise and technical capacity to investigate cybercrime. South Africa is a vulnerable jurisdiction for cyber attacks and has seen an increase in the frequency and severity of incidents over the past few years, ranging from opportunistic cybercrime against SMEs to sophisticated ransomware attacks affecting listed companies and state-owned entities. This is coupled with an evolving cyber insurance market which, as in other countries, is going through a hardening phase with reduced capacity.

Singapore – Nicholas Sykes

It should be unsurprising that cyberrisk, data protection and cyber extortion are three of the top four current risks identified by Asia-based directors and officers. There is similarity and overlap between these three risks, risks which have been significantly increasing over the past few years in Asia, and elsewhere.

Regarding cyberrisk and extortion, in 2020, cybercrime accounted for 43% of overall crime reported in Singapore, and Singapore's Cyber Security Agency has noted a second consecutive year-on-year increase of reported cyber incidents.

Regarding data protection, with Singapore having introduced a mandatory notification regime for data breaches from February 2021, coupled with an increase in the maximum financial penalty to take effect in the near future, we are already seeing a substantial increase in cyberinsurance being purchased as companies seek to manage this growing risk.

The combination of Singapore's data enforcement approach and mandatory breach notification means we are likely to see a further increase in the number of investigations and higher fines, which might prompt organisations to consider their insurance needs in this regard.

Australia – Alec Christie, Reece Corbett-Wilkins and Richard Berkahn

With responses from Australasia and Asia making up 28% of the total responses, the survey gives great insight into what we are seeing, and indeed concerned about, in our region.

Cyber attack, data loss and cyber extortion were ranked as the top three risks for directors and officers in our region by a significant margin. Regulatory risk comes in at number four, which is consistent with what we are seeing on the ground.

Taken together, insight from the survey are a clarion call to all business in our region to:

- Uplift their cybersecurity and privacy compliance activities
- Focus on preparing adequately for a cyber event to occur recognising geo-political factors currently at play in Europe
- Simulate board-level cyber exercises to develop institutional muscle memory and cut through decision paralysis
- Reduce supply chain dependency and third party cyberrisk
- Take out appropriate cyberinsurance cover if they haven't already done so.

Europe – David Meheut

Cyber attacks have come on top of the risks identified by respondents in Europe. This is not surprising. As cybersecurity agencies like ANSSI has reported, the rise in the number of ransomware attacks may have slowed down in 2021 compared to 2019-2020 but remains at a very high level and affects businesses and public organisations of all sizes.

In fact, when one looks in closer detail, the rise on attacks against smaller organisations is still significant. In terms of liability exposures, what may have been initially seen as force majeure may increasingly become a source of liability when managers are questioned about the level of readiness of the organisation under their watch when an attack occurs.

The conflict in Ukraine and renewed geopolitical tensions will bring more tensions, particularly on operators of critical infrastructures. On fines imposed by data protection agencies, the various European countries still have very differing approaches as to their respective sanction policies.

India – Sumeet Lall

Recent data released by the National Cyber Crime Records Bureau shows an 11% jump in cyber crime cases on the previous year and we are seeing a rise in investigations related to data theft, leading to exposures for directors and officers. Cyber events often, but not always, lead to data loss. In this regard, India's proposed new data protection law, which seeks to strengthen and bring standards in line with other jurisdictions and will also see the imposition of hefty fines and penalties for non-compliance of its provisions, remains pending before parliament, with the bill expected to pass later this year. The new law will inevitably lead to a rise in exposures for directors and officers.

Cyber Extortion - ransomware and payment of ransoms

Glyn Thoms, WTW

Cyber risk is still ranked as the most significant risk facing directors and officers, but this year, we asked people also to comment on cyber extortion and it has immediately been ranked in the top four risks across all regions, company revenue sizes and industries.

The concerns around cyber extortion are undoubtedly driven by the surge in ransomware attacks over the last 24 months, the majority of which have included the demand for an extortion payment. Ransomware has become a low investment, low risk and high reward method of cybercrime which organisations cannot ignore. Looking at our WTW Claims Insight Data – where we have reviewed more than 2,000 claims' across our portfolio – we have seen a 200% increase in ransomware claims notifications under cyberinsurance policies since 2019.

200%
increase in ransomware claims notifications under cyberinsurance policies since 2019

From an industry sector perspective, our data shows the top three industry sectors impacted by ransomware attacks are healthcare, manufacturing and education. In 2021, we also saw a shift in tactics from the cybercriminals, including one of the first major attacks against critical infrastructure, the highly publicized Colonial Pipeline attack. As a result, governments and regulators have been alerted to ransomware and extortion activity.

From a cost perspective, our claims data shows the top two cost components following ransomware attack are business interruption (33%) and ransomware payments (22%), with an average ransom demand of $5.5m.

The top two cost components following ransomware attack

Business interruption 32%

Ransomware payments 22%

with an average ransom demand of $5.5m

To pay or not to pay?

When faced with an extortion demand, one of the key considerations for directors and officers is whether or not to pay the demand. In our experience, the discussion around whether to pay is not always straightforward. The board will usually need to consider several factors including:

- **If we don't pay, will we be able to recover our systems and data?** And even if we do pay, does this guarantee we will recover everything?
- **Are we allowed to pay?** Putting aside the question of whether or not to pay, the legality of extortion payments requires careful consideration. The position on legality varies across jurisdictions and there are several financial sanctions and legislative requirements that potentially come into play.
- **If we can pay, how would we pay an extortion demand?** Ransomware attackers often demand ransom payments in cryptocurrency. Therefore, if the decision is taken to pay, it's important to plan how you would access cryptocurrency.
- **Do we have insurance in place and what does it cover?** For companies purchasing specific cyberinsurance, coverage will usually be provided for the financial impacts of a cyber extortion event, including extortion payments, incident response costs, business interruption and regulatory costs and liabilities. Coverage will also usually include access to specialist extortion advisors to support with the investigation and recovery.

The risk of cyber extortion is real, and we have outlined above, the considerations for directors and officers can be complicated. If nothing else, this highlights the need for directors and officers to be aware the exposure and to ensure that their organisation takes a proactive approach to cyber risk identification, quantification, and mitigation.

Climate change, environment and other ESG factors

Laura Cooke and Jane O'Reilly, Clyde & Co

Global overview

The survey results indicate directors' concerns about climate change and the environment have increased in all regions, with the exception of the U.S., which has remained broadly the same. Globally, the risks to organisations' business operations of climate change and the environment ranked as more significant than the geo-political climate (with the exception of Latin America), diversity, equity and inclusion, and Brexit. However, perhaps unsurprisingly given the continuing effects of the pandemic, globally, more immediate risks concerning the economic climate, cyber attacks, COVID-19 and lockdown measures, all ranked higher than or equal to climate change and the environment. Interestingly, the larger the company by revenue, the more significant the risk around climate change and the environment was perceived.

Despite the survey findings, climate and environmental, social, and governance (ESG) risks will continue to increase for directors and officers as governments, regulators and stakeholders seek to bring about the rapid changes required to meet international climate and ESG commitments in the run up to 2030 and beyond.

the larger the company by revenue, the more significant the risk around climate change and the environment was perceived

U.K. and Europe

For the U.K. and European participants, 44% and 52%, respectively, identified climate change and the environment as a 'very significant' or 'extremely significant' risk to business operations, a slight increase on 2021's results, indicating these risks are climbing the corporate agenda. However, when considering the risk that climate change presents to directors, the results fall to 24% of respondents in the U.K. and 33% of respondents in Europe.

The U.K. hosted COP26 in 2021, a 'ratchet' year under the Paris Agreement. COP26 saw sweeping commitments for net-zero by 2050 including a global agreement to 'phase down' use of unabated coal, national alliances, including Wales and Ireland, sounding the end for oil and gas production and exploration licences in certain locations, increased sustainability financing, and biodiversity protection commitments.

Climate change, environment and other ESG factors

Laura Cooke and Jane O'Reilly, Clyde & Co

In the U.K., the Financial Conduct Authority (FCA) has issued a new listing rule, extending its requirements for listed firms to produce climate-related disclosures, aligned with Task Force on Climate-Related Financial Disclosures (TCFD) reporting and wider ESG-related risks and opportunities, on a comply or explain basis.

As the U.K.'s mandatory TCFD-aligned climate disclosure requirements for a broader category of firms come into force in April 2022, the U.K.'s Department for Business, Energy and Industrial Strategy (BEIS) published guidance for those large and listed companies that must start reporting this year.

There is increasing pressure on financial institutions to make climate and ESG-related financial disclosures amid concerns of greenwashing and the need to scale up sustainable investment.

The E.U.'s taxonomy currently requires certain entities to disclose activities related to climate change mitigation and adaptation. This taxonomy and others will likely be a credibility test of 'green' and 'ESG' funds, which will probably see an uptick in liability risk in the Financial Institutions and D&O space. In the meantime, the U.K. is developing its own taxonomy which intends to build on the EU and other international taxonomies.

The increasing focus on reporting at regional and national levels is leading to greater convergence on reporting standards. The emergence of the International Sustainability Standards Board at COP26 aims to draw on the TCFD, SASB and CDSB to provide a common global reporting framework. The increase in reporting obligations is reflected in the survey responses, with 54% of those who indicated that they considered climate change risk for directors to be at least 'significant' stating that reporting requirements, in particular, were 'very or extremely significant'. In the U.K., reporting requirements were ranked as the highest climate-related risk for directors (when compared to Transition risk and Physical risk). We can also observe that different industrial groups rank these obligations differently, with Energy & Utilities considering that reporting requirements by far were the most significant climate-related risk for directors at 74%.

There is also greater focus on protecting natural resources and biodiversity, the value of which often goes unquantified. The Task Force on Nature-related Financial Disclosures has prepared a voluntary disclosure framework which is expected to rapidly develop in the disclosure landscape, with the beta version published in March 2022.

The E.U.'s proposed directive on Corporate Sustainability Due Diligence (CSDD) creates new standards of care and due diligence responsibilities for companies around monitoring supply chains for human rights and environmental harms and to mitigate those harms. The CSDD would have extraterritorial effect which would be significant for businesses operating within the Block and the value chain of EU companies.

As standards and expectations increase, so does the scrutiny and liability risk. In March 2022, the ECB demanded decisive action from the banks it oversees to improve their climate and environmental disclosures, after none had met the ECB's expectations.

In the U.K., the IPCC's latest report, in early 2022, has led to criticism of the U.K. government's insufficient response to climate change and ClientEarth's suit against it for breaches under the Climate Change Act is underway. The case is expected to be heard in the High Court towards the end of 2022.

There has been a consistent stream of climate litigation over the past year in the E.U. and U.K. and we are now starting to see potential derivative actions being pursued against directors personally, alleging failures to divest from fossil fuels and failures to formulate adequate climate strategies.

Companies and their directors and officers should expect increasing scrutiny of their disclosures, business activities and climate strategies from investors, stakeholders, financial institutions, regulators and insurers on matters of climate, the environment and ESG.

Regional views from Clyde & Co

Australia - Jacques Jacobs, Jacinta Stoddard and Dean Carrigan

Australia is at the very tip of the spear in terms of extreme physical manifestation of climate impact. Catastrophic bushfires in late 2019 were followed by unprecedented and severe flooding in eastern Australia in early 2022 which bookended the Australian COVID-19 pandemic experience. Physical climate risks are therefore very much front of mind for most Australian boards.

Local climate-related liability exposure and regulatory risk is also heightened. We expect Australian climate-related litigation and regulatory action will continue to increase, evolve and expand. In particular, we predict activity will jump across the fence from a historical focus on claims against governments and the public sector into the private sector. This will be the case regardless of industry sector and we expect heightened claims activity in the Australian financial services, managed investment, fossil fuel, retail, travel and transport and construction/infrastructure sectors.

Climate change, environment and other ESG factors

Laura Cooke and Jane O'Reilly, Clyde & Co

Businesses and boards will be pursued because of actions and advice they have taken and given, or have failed to have taken, in relation to climate risks. In the public entity environment, this might include mass tort-based claims or securities class actions stemming from alleged inadequate climate transition planning and inadequate climate-related disclosure.

Australian regulators have recently been publicly vocal in warning businesses against greenwashing and engaging in misleading and deceptive practices relating to climate-related advertising and making 'green' representations, including in financial disclosures.

Australia is a highly litigious jurisdiction. The plaintiff bar and the many established litigation funders operating here are actively exploring climate-related claims against Australian businesses and their boards

Hong Kong – Mun Yeow

Hong Kong is a leading international financial centre and has a significant role to play in developing a global green and sustainable finance strategy, having been among the earliest cities in Asia to address and combat climate change. As a direct response to the Paris Agreement, Hong Kong released the Climate Action Plan 2030+ in 2017 and an updated Climate Action Plan 2050 in 2021.

Having already made moves towards decarbonization, Climate Action Plan 2050 clearly sets out the target of reducing total carbon emissions by half before 2035 from the 2005 level and achieving carbon neutrality before 2050. The strategy covers net-zero electricity generation, energy saving and green buildings, green transport and waste reduction. Hong Kong plans to allocate about US$30 billion in the next 15 to 20 years to implement mitigation and adaptation measures to combat climate change.

By 2025, climate-related financial disclosures within the TCFD framework across all relevant sectors will become mandatory. Hong Kong will be one of the first jurisdictions in proposing and implementing laws and regulations to mandate TCFD-aligned financial reporting.

To assist, the Hong Kong Monetary Authority has issued draft guidelines on managing climate-related risks by authorised institutions, while the Securities and Futures Commission has issued a consultation paper on managing and disclosing climate risks by fund managers.

South Africa – Daniel Le Roux

South Africa's heavy reliance on fossil fuels to power an ageing and overstretched national grid is plainly unsustainable in light of the COP26 outcomes and the Government's ambition to follow a "just transition" plan away from coal in favour of renewable energy using concessional finance.

This has prompted shareholder activism against banks and lenders in relation to fossil fuel projects and investments, and a moratorium by some lenders on support for such projects.

We anticipate this may produce claims against D&Os where ESG-related commitments are not followed.

There is also the prospect of increased regulatory action against companies and D&Os for inaccurate market disclosures and pollution/contamination claims.

Europe – Henning Schaloske

In this year's survey, climate change does not yet make in the top seven risks for Europe, but that will most likely change. Following COP26, increased regulation as part of the ongoing transition will be incoming, driving both the need to adapt business models and to respond to ESG requirements more broadly.

The landmark ruling in the Netherlands in May 2021, and further climate change actions against companies and directors following on the back of it across Europe, are testament to the fact climate change is a boardroom issue and companies need to address exposures, including increasing liability risks.

Climate change, environment and other ESG factors

Laura Cooke and Jane O'Reilly, Clyde & Co

U.S. - Tim Sullivan

Climate change is a growing risk priority for North American organizations and their various internal and external stakeholders. However, survey respondents in North America placed less emphasis on climate change risks compared to their counterparts in other regions of the world. When asked about the significance of climate change to their business, 34% of respondents in North America categorized such risks as either 'very significant' or 'extremely significant', the lowest ranking by geographical region.

When asked how significant such risks are to the directors and officers of their organization, only 18% of North American respondents classified climate change as a 'very significant' or 'extremely significant' risk, a score 7% less than the average ranking of climate change risks for all regions.

While climate risk is growing in prominence, it does not yet appear within the top seven risks identified by North American survey respondents. However, it is possible that this may soon change, particularly within the U.S..

In response to the growing interest in ESG investing and investor demands for greater transparency, the SEC has taken a series of actions that may result in greater scrutiny of U.S. organizations and their approach to climate-related risks.

Over the past year, the SEC has created a Climate and ESG Take Force within its Division of Enforcement and has included climate-related risks amongst its top examination priorities.

Most recently, SEC Chair Gary Gensler announced in March the Commission will meet publicly to consider staff proposals to mandate climate risk disclosures by public companies.

While it is early in the process, these actions by the SEC may cause U.S. organizations to place even greater emphasis on climate risks.

From an industry perspective, aside from the Energy & Utilities sector, climate-related risks rank higher within the Finance & Insurance industry than it does within all other industries included in this survey. Of those respondents within the Finance & Insurance industry, 50% ranked climate change as either a "very significant" or "extremely significant" risk from the perspective of their organization's directors and officers. When compared to the responses from all industries, the Finance & Insurance industry ranked climate risks 9% higher in significance than the average response of all industry participants. The prominence of climate-related risks within the Finance & Insurance industry may be due, at least in part, to the fact that banks and insurance companies have been subject to climate-related stress tests, particularly in the U.K. and Australia, and various rules and regulations have been proposed or implemented (primarily outside the U.S.) that will impact the Finance & Insurance industry. The growing demand for ESG investing and pressure from climate activists may also be a contributing factor. As the SEC moves forward with its own rules and regulations in the U.S., climate-related risks are likely to garner even more attention from directors and officers in the years ahead.

Insolvency

Mark Sutton, Clyde & Co

Insolvency risk does not feature in the top five concerns for respondents but, nonetheless, globally, 31% considered it a 'very' or 'extremely significant' risk for directors and officers and that concern has grown since the previous survey was undertaken.

It is felt most keenly by those in the transportation and retail industry, which is no surprise given the significant impact the pandemic has had on these sectors.

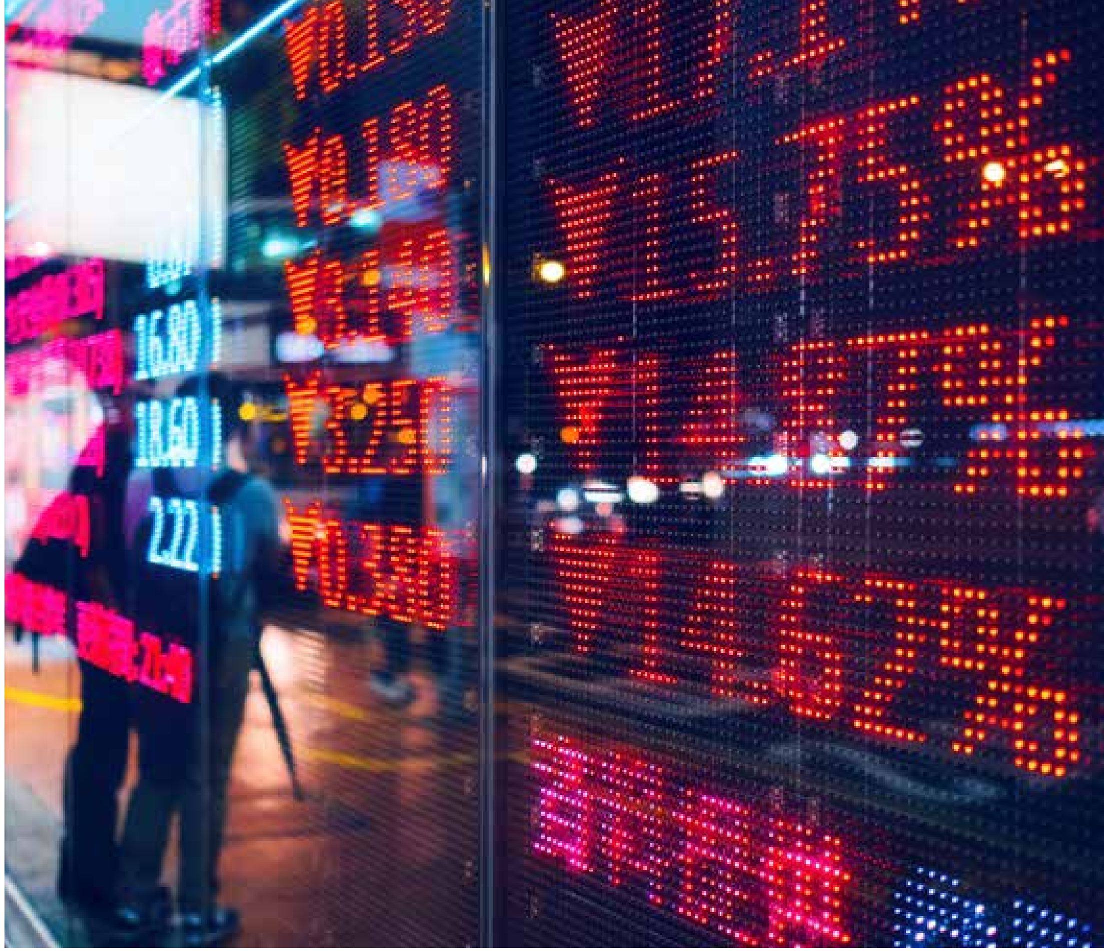
Most countries implemented emergency legislation, providing financial support and relaxing insolvency rules in order to allow companies to navigate the difficult circumstances. This translated into record low numbers of insolvencies in 2020 and through to mid-2021.

In the U.K., statistics show Creditors' Voluntary Liquidation numbers are currently more than double the level in February 2021 and are 40% higher than pre-pandemic levels. However, the number of other insolvency procedures, such as compulsory liquidations for companies and bankruptcies for individuals, remains very low.

It is our view that now government protections have largely ceased numbers will rise and we can expect a greater number of filings in the coming months and years.

Claims against directors and officers related to insolvency events are common and already represent a large risk exposure. Insolvency practitioners are duty-bound to closely examine the decisions and conduct of the directors and senior management in the period leading up to insolvency, which could see the directors and officers investigated for breach of duties to the company and for breaches of company and insolvency legislation.

Further, during difficult economic times, there is a higher risk of fraudulent, dishonest or wrongful actions. Liability in relation to any of these breaches is not only grounds for disqualification but can also lead to actions against directors for the recovery of any sums lost by the company. There may also be claims by the bodies which regulate pensions if the directors' actions negatively impacted the company's pension.



In the U.K., an Act was recently passed which further widens the potential for liability following an insolvency, the Rating (Coronavirus) and Directors Disqualification (Dissolved Companies) Act 2021. This Act provides that existing and former directors can be subject to disqualification even after a company has been dissolved and, if creditors have suffered financial loss due to the director's actions, an order can be made for the director to be personally responsible for those losses.

The aim is to prevent companies from being dissolved (rather than going through a formal liquidation process) with outstanding debts and liabilities, only for the company to be re-established under a new name, a process known as phoenixism.

The Government considers there is a particular risk that some companies will seek to dissolve the company in order to avoid repaying government loans given during the pandemic, such as the Bounce Back Loan. The Act does away with the previous need for the company to be restored to the register, meaning that we can expect an increase in the number of investigations against directors and officers.

Insolvency

Mark Sutton, Clyde & Co

Regional views from Clyde & Co

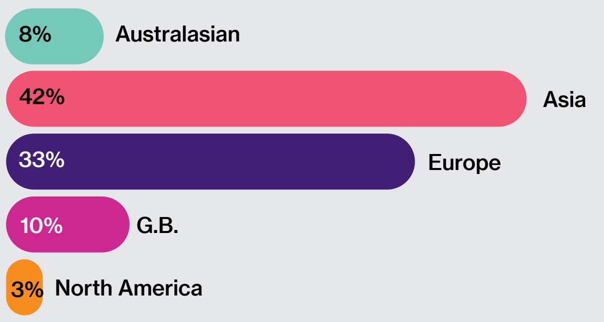
Australia - Christopher Smith

Corporate insolvencies have been falling year on year in Australia since 2016. Last year was again one of the quietest years in memory for many in the field of insolvency and restructuring. The tsunami of insolvencies predicted at the start of the pandemic in 2020 has not materialised. This is due in large part to temporary legislative relief, government support, rent deferrals and leniency from creditors and tax office enforcement, much of which will end soon.

Ironically, as the economy bounces back, the number of insolvencies is likely to increase. Challenges ahead include a shortage of employees, global supply chain issues, and increasing interest rates. The consensus is there will be an uptick in insolvencies at some future point, but perhaps not on the scale envisaged at the start of the pandemic.

Sentiments expressed in the survey reflect the low priority afforded to insolvency in Australia. Only 8% of Australasian participants indicated insolvency, bankruptcy, or corporate collapse risk was ‘very significant’ or ‘extremely significant’ to directors. This was significantly lower than participants in some other regions (Asia 42%, Europe 33%) but on par with others (G.B. 10%, North America 3%).

Insolvency, bankruptcy, or corporate collapse



Percentage perceived the risk ‘very significant’ or ‘extremely significant’ to directors

Source: Directors’ Liability Survey 2022

France – David Meheut

Like in almost every other region, the economic climate has come out as one of the top two risks for organisations’ business operations. This it is unlikely to change given the current geopolitical crisis and the resulting supply chain disruption and inflation, in a climate which was already under stress due to the pandemic.

In terms of the translation of that risk into D&O exposures, with the COVID-19 crisis, it was widely expected insolvency risks would be on the rise in 2021, especially as claims against directors have become more systematic in certain jurisdictions.

However, in most European countries, the filings for insolvency have been much lower than expected, and even decreased in certain countries, largely due to financial supports and schemes put in place by the various governments. With the increased tension, things may change.

India – Sumeet Lall

As with many other countries, the Central government in India took steps to avoid enterprises from being pushed into insolvency during the pandemic, increasing the threshold to initiate insolvency proceedings and suspending the initiation of the insolvency process.

Despite the suspension now having been lifted, the number of applications has not dramatically increased, potentially due to the multiple subsequent waves of the pandemic which affected the ability of the Adjudicating Authority to hear such cases.

The Adjudicating Authority has now recommenced its functioning and a surge in applications is anticipated. Moreover, recent amendments to the insolvency regulations require resolution professionals to report their opinion and determination in respect of avoidance transactions, namely, preferential transactions, undervalued transactions, extortionate credit transactions, fraudulent trading and the like to the Insolvency and Bankruptcy Board of India.

Consequently, a resolution professional is now duty-bound to actively find out if a corporate debtor has been subject to the aforesaid avoidance transactions. Accordingly, it is anticipated the number of proceedings alleging avoidance transactions against directors and officers is also going to increase and there exists a significant risk in this regard.

Insolvency

Mark Sutton, Clyde & Co

Spain – Ulysses Grundey

The recent extension (until 30 June 2022) of a measure to waive the obligation for companies that are in a situation of bankruptcy to file for insolvency proceedings, seeks to hold back a wave of potential business failures. But although the expectation is that the economic situation will improve, according to data from the Bank of Spain one in five companies is at risk of insolvency due to the impact of COVID-19. In addition, a reform of the current insolvency law is on the way which will add obligations to an already very complex law.

South Africa – Graeme Griffiths

COVID-19 has undoubtedly had a substantial impact on the solvency of businesses in South Africa over the last two years. The impact was not just felt in the small, medium, and micro enterprises (SMME) sector, which employs up to 70% of South Africa's workforce, but also amongst well-established corporates which were also forced to implement severe cost cutting measures to thwart the risk of liquidation.

From April 2020 to September 2021, South Africa's official unemployment rate jumped from 23.3% to 34.9%. This equates to approximately 3.3 million more South Africans being unemployed (7.6 million in total), a significant proportion of which can be attributed to retrenchments or business liquidations.

South Africa saw a spike of liquidations in 2020, which from January 2021 to date is now fortunately following a downward trajectory as economies around the world recover. This is hopefully one sign the most severe short-term financial impacts of COVID-19 appear to be behind us.

U.A.E. - Mark Beswetherick

Insolvency regimes across the region are still in their infancy and we have not yet seen a raft of insolvencies or litigation following the financial fallout from the COVID-19 crisis.

However, in a landmark bankruptcy case judgment issued on 10 October 2021, the Dubai Court of First Instance has held the directors and managers of an insolvent Dubai-based Public Joint-Stock Company to be personally liable to pay the outstanding debts of the previously listed company (now in liquidation) pursuant to the U.A.E. Bankruptcy Law.

This decision represents a very significant milestone in the U.A.E. insolvency landscape since the enactment of the Bankruptcy Law in late 2016, being the first known instance of a case where such personal liability has been ordered.

The approach taken by the Dubai Court has also confirmed that duties of directors and managers of a U.A.E. company are clearly owed towards the company's creditors. However, this approach is the subject of a current appeal for which the decision is awaited with interest.

Regulatory exposures

Mandip Sagoo, Clyde & Co

While concern about regulatory risk has dropped this year amongst respondents when compared with last year's survey (though still remaining in the top 5), the level of risk posed to companies and their directors and officers is considerable. This is evidenced by 20% of respondents having experienced a regulatory claim involving a director, the figure rising to 34% for very large revenue companies. Companies in Europe, excluding the U.K., saw the largest percentage of such claims (26%) and, unsurprisingly, financial services firms experienced the most actions.

Regulatory requirements are ever-expanding and the chance of falling foul of the myriad of rules is considerable, especially in this era of accountability. Financial regulators in particular are taking a very proactive stance and are keen to stress any drop in activity related to the pandemic was temporary. They are focused on tackling traditional risks, such as market abuse and anti-money laundering failures, in addition to emerging issues, such as climate change-related risks.

Another area of focus is addressing the inadequacies highlighted by the pandemic, especially in relation to systems and controls, contingency planning and operational resilience.

Consumer protection remains a key priority in many jurisdictions with the Financial Conduct Authority (FCA) in the U.K., for example, proposing a new consumer duty. This presents not only an operational challenge and shift in approach to dealings with consumers, but the potential for further regulatory action against firms and senior management.

There is also growing pressure to expand current corporate criminal liabilities so wrongdoers are held to account and to encourage companies to take more responsibility for the culture they foster within their organisations.

In the U.K., this includes examining whether the identification principle needs to be reformed. This is where, in order for the company to be held liable, a prosecutor must prove the individuals involved in the crime represent the "directing mind and will" of that company, that is, the individual's actions are to be considered those of the company.

This is very difficult to establish and has led to a low number of convictions for which U.K. prosecutors, have been criticised. Reforms could pave the way for an increased risk of prosecution for corporates and directors and officers.

Regulatory exposures

Mandip Sagoo, Clyde & Co

It is not just prosecutors such as the Criminal Prosecution Service and Serious Fraud Office, that are seeking to hold companies and directors and officers criminally accountable. The FCA recently levied significant fines on banks for AML failures, including pursuing a bank under its criminal powers, securing a conviction and imposing a fine in excess of £265 million. In addition, regulators such as the Pensions Regulator, are increasingly taking a forceful approach, armed with new powers that could see companies and their D&Os face significant penalties, including criminal sanctions.

Cyber risk and data loss remains a large regulatory/administrative exposure. Whilst cyber attacks do not always lead to data loss and data loss can occur without a cyber event, the two are often inextricably linked, especially given how cyber risk has evolved in recent years, with a sharp increase in ransomware attacks that now often feature exfiltration of data and extortion.

Record fines are being imposed by data protection authorities and cybersecurity failings are being identified and sanctioned by sector regulators. The U.K. is no exception – large fines are being imposed for data protection failings and sector regulators are striving to improve firms' cybersecurity and operational resilience, through close supervision and proactive enforcement.

With the crisis in Ukraine, there is the possibility of a rise in investigations and enforcement action linked to breaches of sanctions and other regulations.

All in all, the landscape remains a challenge for directors and officers and we expect this to increase as regulators continue in their endeavours to establish frameworks designed to encourage corporate and individual responsibility, in the pursuit of market confidence and consumer protection.

Regulatory exposures

Mandip Sagoo, Clyde & Co

Regional views by Clyde & Co

Australia – Avryl Lattin

In Australia, we have now seen the implementation of the final tranche of legislation flowing from the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry. Although there is sense of relief the reform agenda has slowed, participants in the financial sector will need to continue to adapt their product offering and customer approach to meet the new regulatory environment. Across all sectors, companies will need to take into account the increased frequency of regulatory enforcement action and higher penalty regimes.

Hong Kong – Rosie Ng

The Securities and Futures Commission's (SFC) proactive and "front-end loaded" approach in pursuing corporate misfeasance, led to a number of investigations and sanctions in 2021, including the Court of Appeal's success in obtaining a compensation order of HK$622 million against former directors of a company for due diligence failures and large-scale misapplication of company funds. The trend continues upwards. As insolvencies continue to increase, stakeholders will likely continue to challenge management decisions leading to more shareholder activism.

The Stock Exchange of Hong Kong (SEHK) amended the Listing Rules (with effect from 3 July 2021) to impose secondary liability on "Relevant Parties", to include senior management (as newly defined), who by act or omission cause or knowingly participate in a breach of the Listing Rules. Further, the SEHK's new Corporate Governance Code on ESG and gender diversity, which came into effect in January 2022, has broadened the duties of directors of issuers and of IPO applicants in this regard.

Spain – Ignacio Figuerol

Criminal and regulatory investigations remain a major exposure in relation to bribery and corruption, health and safety, money laundering and environmental issues, and are increasing in relation to data protection and competition matters. In addition, the new scenario arising from the sanctions imposed by the U.S. and E.U. on Russia are likely to give rise to issues and investigations with a wider reputational impact.

India – Sumeet Lall

In India, various investigative agencies have been set up by the central government to ensure regulatory compliance. Active agencies include the Enforcement Directorate which is conferred with wide-ranging powers to investigate and prosecute corporates for offences relating to money laundering and violations of the Foreign Exchange Management Act.

The Enforcement Directorate has come down heavily on cryptocurrency exchanges, with seven ongoing investigations relating to cryptocurrency-related money laundering and the related attachment of assets over INR 135 crore (USD 17.7 million approximately).

Climate change has recently found a place in active discussions between the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI). The RBI has insisted on incorporating climate risks into commercial banks' risk and compliance strategies as one of its future goals. Further, SEBI has instructed the top 1,000 listed entities by market capitalization to implement new sustainability-related reporting requirements.

Companies need to carefully manage compliance with applicable rules and regulations that could open up an increased risk of inspection and prosecution by investigative agencies or regulator

Directors and officers insurance coverage

Angus Duncan, WTW

In addition to asking respondents to answer questions on risks for directors, we also asked them to comment on the directors and officers insurance their organisation purchases and their corporate indemnification arrangements.

72% of our clients responded their organisations indemnified their directors to the fullest extent allowed by law, while 11% said the indemnification was only where approved by shareholder vote. Of course, this can be a key issue in some directors and officers claims, particularly for policies that look only at the question of whether the company is required or permitted at law to indemnify directors.

We also asked respondents to rank the value they see in various aspects of their directors and officers cover. The highest values went to understanding how directors and officers claims will be controlled and settled and a choice of lawyer-counsel. The lowest values went to the extent to which clawback provisions apply to the policy and whether there is coverage to appoint a public relations expert to manage reputation risk in the event of a claim. These last two were the lowest ranked in last year's survey as well.

Looking at the regional split of the responses, we can see all regions except Asia ranked these two as the least significant, except in Asia where having a broad definition of who is insured ranked second lowest with reputation risk cover coming in third lowest.

Handling and settlement of claims was number one in all regions except North America, where it was choice of lawyer, and Latin America, where it was cover for fines and penalties.

Directors and officers insurance coverage

Angus Duncan, G.B.

In terms of choice of defence counsel, only 18% of respondents ranked cost as being an important factor while 92% said “Expertise in Field” was an important factor.

Turning to policy limits, retentions and premiums, only 11% of respondents had seen reductions in their policy limits over the last year, with just 2% saying they anticipated a reduction next year.

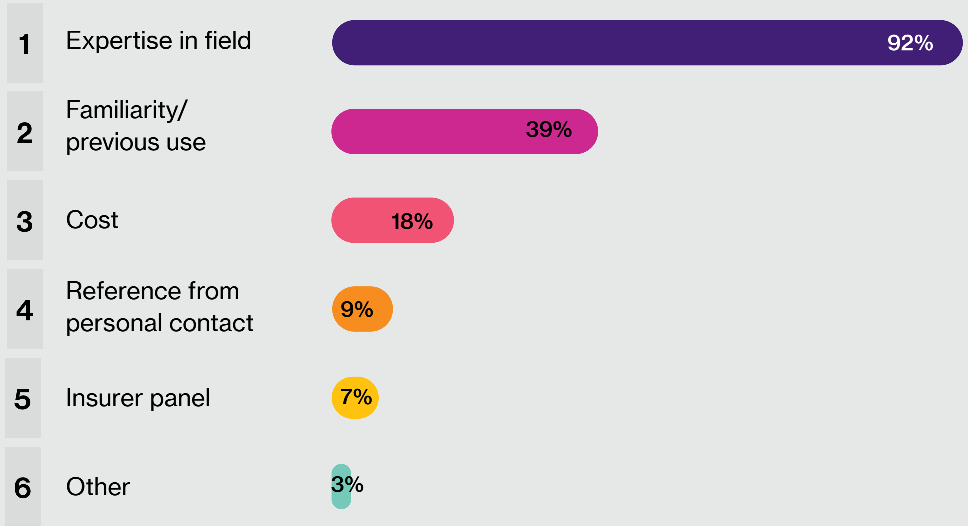
By contrast 64% had seen an increase in premium and 44% anticipated an increase next year. Of those who had seen their limits change, 44% said this was down to increased cost while 44% said it was down to availability of capacity.

The limits of liability being purchased by the respondents’ organisations also varied remarkably. While most companies with revenue of $5bn or more purchased at 100+millions of directors and officers insurance, 13% purchased only 10-19million and 1% purchased only 4-9 million.

By contrast, 2% of organisations between $1bn to $5bn revenue purchased no directors and officers insurance, which rises to 6% for organisations with revenues between $50m to $1bn and 16% for organisations with less than $50m in revenue.

Defence counsel

What are/would be the most important factors in choosing lawyers/counsel in connection with any particular claim or investigation?



Note: Top 2 answerers
Source: Directors’ Liability Survey 2022

Insurance coverage issues – by region

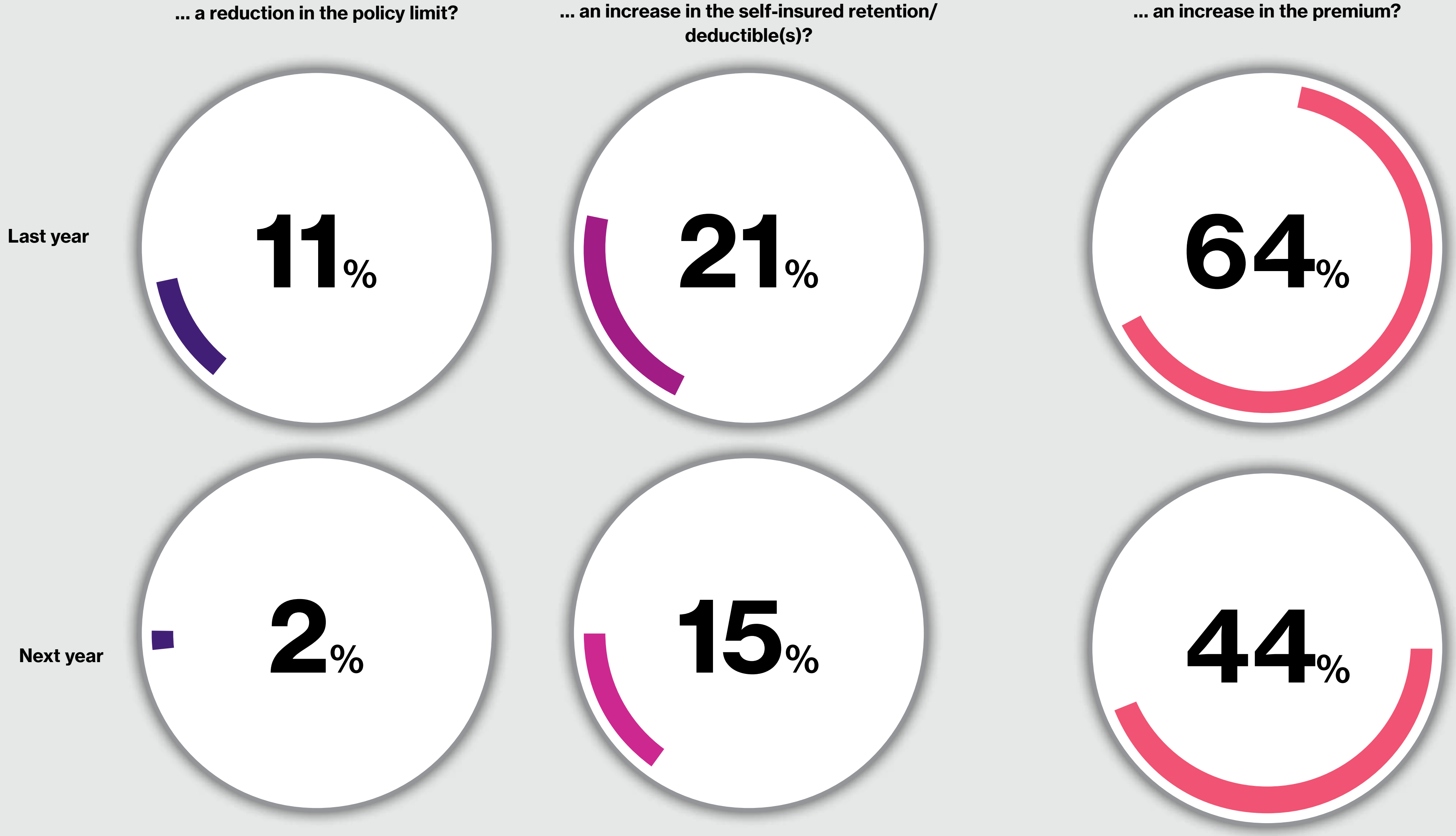
How important are the following Directors & Officers liability insurance coverage issues to you?

Country of office	Europe	G.B.	Asia	LatAm	North America	Australasia
How claims against the Directors and Officers will be controlled and settled	69%	58%	62%	67%	78%	75%
A choice of lawyer/counsel	69%	36%	51%	77%	81%	64%
Whether your D&O policy and/or company/organisation indemnification will be able to respond to claims in ALL jurisdictions	63%	43%	62%	62%	82%	42%
Whether there is cover for fines and penalties	63%	46%	48%	56%	83%	51%
Whether there is cover for cost of legal advice at the early stages of an investigation	65%	43%	51%	41%	80%	64%
Understanding how coverage disputes between you, your company/organisation and your insurers will be dealt with	63%	51%	38%	59%	75%	61%
How the cover responds in the event of conflict of interest or claim between a Director and the company/organisation	60%	40%	52%	44%	78%	47%
A broad definition of who is insured including most categories of employees	62%	46%	35%	56%	76%	56%
The extent to which clawback provisions apply to the policy	50%	28%	28%	38%	71%	42%
Whether there is coverage to appoint a public relations expert to manage reputation risk in the event of a claim	42%	17%	35%	35%	73%	39%

(% of 'very' or 'extremely important')
Source: Directors' Liability Survey 2022

Insurance coverage issues – by region

How have the following aspects of your organisation's Directors & Officers liability insurance policy changed or are expected to change



Note: Don't know was excluded
Source: Directors' Liability Survey 2022

Corporate culture and whistleblowing

Lawrence Fine, WTW

While 73% of respondents to the survey said they knew what their organization's whistleblowing policy is, only 24% said they thought their organization's culture is affected by the whistleblowing policy.

This is down from 35% in 2021, which is quite surprising considering that in FY 2021, the SEC's Office of the Whistleblower (OWB) awarded approximately $564 million to 108 individuals, representing both the largest dollar amount and the largest number of individuals awarded in a single fiscal year.

When compared with the entirety of the whistleblower program, FY 2021's results further stand out: from the inception of the program in FY 2011 through FY 2020, the commission made approximately $562 million in whistleblower awards to 106 whistleblowers. This means the commission made more whistleblower awards in FY 2021 than in all prior years combined.

The awards made in FY 2021 also included the commission's two largest awards to date – a $114 million award to one whistleblower and a combined $114 million award to two other whistleblowers. The SEC stated: "These large awards underscore the Commission's commitment to rewarding whistleblowers who provide specific and detailed information that plays a significant role in the success of the agency's enforcement actions."

In FY 2021, the OWB also processed more claims than in any other year of the program and issued the largest number of Final Orders resolving whistleblower award claims, including both award and denial orders. The Commission issued 318 Final Orders for individual award claims.

Corporate culture and whistleblowing

Lawrence Fine, WTW

Another record-breaking year for whistleblower tips

FY 2021 featured the largest number of whistleblower tips received in a fiscal year since the program's inception. In FY 2021, the Commission received more than 12,200 whistleblower tips, an approximate 76% increase from FY 2020, the second highest tip year, and a more than 300% increase since the beginning of the program.

As in prior fiscal years, tips received this fiscal year came from a variety of geographic origins, both domestic and foreign. The commission received tips from individuals in 99 foreign countries, as well as from every state in the U.S. and the District of Columbia.

As a result of all of the above, it can be assumed if you are a U.S. company and something is going on there which might be of interest to the SEC, one of your employees is likely to be lured into reporting the situation in the hopes of resulting lucrative rewards. Consequently, this situation might warrant greater concern from U.S. officers and directors.

The outlook ahead

All of the whistleblowing enforcement and recovery actions discussed above were accomplished under the previous administration. Meanwhile, with the change of administration, there is reason to expect substantially more aggressive regulatory enforcement going forward. Gary Gensler, the Chair of the SEC, and Deputy Attorney General Lisa Monaco, both of whom were sworn in last April, have been clear and forceful in their early public statements.

Deputy Attorney General Monaco has said: *"Accountability starts with the individuals responsible for criminal conduct . . . this department's first priority in corporate criminal matters [is] to prosecute the individuals who commit and profit from corporate malfeasance." Also, "[C]corporate culture matters. A corporate culture that fails to hold individuals accountable, or fails to invest in compliance — or worse, that thumbs its nose at compliance — leads to bad results."*

Deputy Attorney General Monaco stated that, *"to be eligible for any cooperation credit, companies must provide the department with all non-privileged information about individuals involved in or responsible for the misconduct at issue. To be clear, a company must identify all individuals involved in the misconduct, regardless of their position, status or seniority."* Furthermore, *"all prior misconduct needs to be evaluated when it comes to decisions about the proper resolution with a company, whether or not that misconduct is similar to the conduct at issue in a particular investigation."*

See https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-gives-keynote-address-abas-36th-national-institute

Gensler also stressed accountability, individual and corporate, as a top priority, saying, "when it comes to accountability few acts rival admissions or misconduct by wrongdoers". He also said that pursuing "high-impact cases" is important because such stories can help "pull many other actors back from the line". On the subject of "the line", Gensler offered the following suggestion: "So if you're asking a lawyer, accountant, or adviser if something is over the line, maybe it's time to step back from the line. Remember that going right up to the edge of a rule or searching for some annuity in the text or a footnote may not be consistent with the law or its purpose". SEC Chair Gensler mentioned a particular focus on SPACs, cyber, crypto, and private funds, promising to examine the "economic realities of a given product or arrangement to determine whether it complies with the securities laws". https://www.sec.gov/news/speech/gensler-securities-enforcement-forum-20211104

As a consequence of the increasingly aggressive stance of the SEC and DOJ, it seems likely that U.S. directors and officers will rate regulation higher in their hierarchy of concerns next year.

Corporate culture and whistleblowing

Regional views by Clyde & Co

Australia – Alena Titterton

The last year on corporate culture in Australia has been overwhelmingly focused on the approach that organisations take to sexual harassment, discrimination and misconduct. Recent allegations highlighted in the media about inappropriate workplace behaviours, sexual harassment and generally poor workplace cultures in places like the Australian Federal Parliament, the High Court of Australia, the Victoria Supreme Court and high profile listed companies, shows just how pervasive this problem unfortunately continues to be. But these are not isolated instances. It remains far more prevalent than some people may appreciate. This has been a high profile issue in Australia following the release of the Sex Discrimination Commissioner's Respect@Work Report and the Federal Government's somewhat delayed response to that Report. The Sex Discrimination and Fair Work (Respect at Work) Amendment Bill 2021 has implemented some of the recommendations of the Respect@Work Report (for example, making it clear that harassing a person on the basis of sex is prohibited). While the key recommendation to introduce an express positive duty of care on employers to take reasonable and proportionate measures to eliminate sex discrimination and sexual harassment has not yet been implemented, it is something that directors and officers can expect to see in law reform in the year ahead.

Given that background, it is perhaps unsurprising to see the survey results in Australia on the corporate culture questions finding less focus on whistleblower policies, both in terms of understanding of the organisation's policy Only 38.89% of Australian respondents indicated they knew their organisation's whistleblowing policy to a great extent, compared to 73% of respondents globally.

Also, potentially unsurprising is how much the organisation's culture is affected by this policy, with only 2.78% of Australian respondents indicating the whistleblower policy affected culture to a great extent, compared to 24% of respondents globally.

Of course, whistleblower policies are a part of the picture in maintaining effective systems and processes for positive corporate cultures. However, in the Australian context these policies are not the focus in how directors and officers in the region are currently grappling with improving corporate culture in practice.

Europe – Ignacio Figuerol

The E.U. Whistleblower Protection Directive was to be implemented by the EU Member States by 17 December 2021, but only a limited number of states have implemented it so far. At the same time, companies in the private sector with 250 employees or more shall comply by 17 December 2021, whilst smaller entities with 50-249 employees have an additional two-year period until 17 December 2023.

In addition, on 4 March 2022 the European Commission announced the introduction of the E.U. Sanctions Whistleblower Tool. According to the Commission, the tool can be used to report on, "past, ongoing or planned" E.U. sanctions violations, as well as attempts to circumvent these. Therefore, we are yet to see to what extent this has a real impact across Europe.

On the other hand, the E.U. Commission published on 23 February 2022 a proposal for a directive on corporate sustainability due diligence obligations to foster sustainable and responsible corporate behaviour throughout global value chains. The proposal also introduces duties for the directors of the E.U. companies it covers.

The proposed directive refers to the setting up and overseeing of the implementation of the due diligence processes, as well as integrating due diligence into the corporate strategy. Company directors shall take into consideration all type of consequences of their decisions for sustainability matters, including climate change and environmental consequences and other factors.

Spain – Ulysses Grundey

As set out above, 17 December 2021 marked the deadline for countries to complete the transposition of European Parliament Directive (E.U.) 2019/1937, also known as the 'whistleblowing directive'.

Among other things, the legislation provides for the creation of whistleblowing channels to effectively protect whistleblowers who report everything from potential money laundering to breaches of environmental legislation.

This is a challenge for many clients who now have a deadline until 17 December 2023 to comply with the new legal environment and implement a channel for whistleblowing.

Employment practices liability exposures – COVID-19's lingering impact?

Joann Nilsson, WTW

We have slowly begun to emerge from the pandemic and over the past two years we have seen the impact of COVID-19 affect all sectors of society. 59% of all survey respondents around the world view COVID-19 and lockdown measures as either 'very' or 'extremely important' and it remains a topic of interest for directors and officers.

While each region in the survey found COVID-19 and lockdown measures were a 'very significant' or 'extremely significant' risk for their organization's business operations, in North America 62% of individuals surveyed believed COVID-19 and lockdown measures were either 'very significant' or 'extremely significant.' This was the third largest risk after economic climate and cyber attack.

The focus respondents gave to COVID-19 and lockdown measures is not surprising, with the U.S. having seen vaccine mandates implemented by the Government and subsequently challenged in the court system, until a recent ruling was eventually issued by the U.S. Supreme Court.

One of the most intensely scrutinized matters in the second half of 2021 was the Department of Labor's Occupational Safety and Health Administration's (OSHA) COVID-19 Vaccination and Testing Emergency Temporary Standard (ETS). This would have mandated COVID-19 vaccinations or at least weekly testing for workers at companies in the U.S. with 100 or more employees by January 4, 2022, subject to legally required accommodations. On January 13, 2022, the U.S. Supreme Court issued a stay of OSHA's ETS.

Employers not covered by another federal, state, or local mandate may choose to implement whatever policies and practices are best suited to the unique needs of their workplace.

Employers choosing to maintain workplace vaccination policies must still follow other applicable laws, such as Title VII and the Americans with Disabilities Act, and be cognizant of the requirements in their specific state, as several states have enacted measures that either restrict or impact vaccination requirements.

Employment practices liability exposures – COVID-19's lingering impact?

Joann Nilsson, WTW

Many of the EPL claims coming out of the pandemic have been in relation to failure to accommodate based on religion or disability. A religious or medical accommodation is often requested by an employee when a conflict arises between a specific task or position the employee cannot fulfill due to a medical or religious reason.

Today, this means a vaccine mandate may create the need for an accommodation where an employee cannot fulfill that requirement due to medical or religious reasons and this is an issue which employers will need to navigate through the guidance of legal counsel.

While COVID-19 claims continue to manifest, these are not the only employment claims companies are facing, with 35% of respondents saying they found the risk of employment claims for their directors and officers (whether reputationally or financially) 'very significant' or 'extremely significant'. This risk was highest in the energy and utilities sector at 40%. By slight contrast, in our 2021 survey, 38% of respondents found the risk of employment claims 'very or extremely significant.'

In addition to COVID-related claims, we anticipate the following factors may lead to increases in employment claims throughout 2022:

- In 2021 various states and localities passed new laws restricting the use of non-competition agreements. On a federal level, the Federal Trade Commission is considering whether to exercise its rule making authority to curtail use of non-compete clauses.
- As return-to-work and hybrid scheduling continues in 2022, considerations around how employers monitor productivity without breaching privacy and confidentiality issues may become a bigger issue.
- We may see more court filings of claims of sexual assault or harassment. Recently, President Biden signed into law the Ending Forced Arbitration of Sexual Assault and Sexual Harassment Act of 2021. The Act amends the Federal Arbitration Act (FAA) to give employees who are parties to arbitration agreements with their employers the option of bringing claims of sexual assault or sexual harassment either in arbitration or court.

G.B. - Chris Holmes

It is notable the perception of risks for directors and officers in relation to return to work/ COVID-safety/vaccination status is relatively low for G.B. at 11%. This compares with 25% for Europe and 38% for North America, and 51% for Asia.

The statistics also show COVID-19 and lockdown measures were ranked at 47% in terms of significance for G.B., which is the lowest percentage ranking amongst the regions and perhaps due to the U.K. Government's approach to lifting lockdown restrictions and its plans for living with COVID.

The perception of risks for directors and officers in relation to risk of employment claims is also relatively low for G.B. at 14%, in comparison to 28% for Europe, 38% for North America, and 50% for Asia. This may be related to differing employment claims cultures and/or employment protection regimes across the regions.

Key employment-related perceived risk areas for businesses in G.B. include data protection/loss, health and safety, regulatory risk, and climate change issues.

From our experience, diversity, equality, and inclusion are further key employment-related areas of focus for businesses operating in the region.

G.B. - Richard Multon

In terms of the London insurance market, EPL is still very much an ancillary line alongside D&O. Although there have been a few new markets to announce that they will now consider writing EPL, they will only do so alongside participation of the D&O. More appetite for excess layers is appearing, but is heavily dependent on retention level, sector, attachment point, and exposure to the U.S.

Use of alternatives to the commercial insurance market for D&O liabilities

Angus Duncan, Lawrence Fine and John Orr, WTW

The steep increase in the price of insurance over the last two-three years has led to a lot of discussions about potential alternatives which might be available for D&O liabilities other than purchasing a D&O insurance policy from the commercial insurance market.

Potential solutions include using a captive insurance vehicle for some or all of the corporate reimbursement cover ("Side B") or company securities claims cover ("Side C"), using a captive insurance vehicle (in the form of a Protected Cell Company ("PCC") or a Segregated Account Company ("SAC")) for some or all of the non-indemnified loss cover ("Side A") ; establishment of an indemnification trust; a personal guarantee of director liabilities from the CEO or a major shareholder; and other more bespoke solutions.

While the use of captives for Side B or Side C has been done in a number of situations, in our experience, the Side A solution has tended to be more expensive than simply purchasing insurance from the commercial D&O market. However, in our survey, marginally more respondents indicated their organisation had used a captive insurance vehicle for Side A (6%) than for Sides B/C (5%). A further 18% and 20% (respectively) were considering doing so in the future.

The use of a personal guarantee from the CEO or other major shareholder saw some fairly high-profile examples between 2020-21 and, in fact, more of the respondents indicated this was in place (7%) than for either type of captive solutions.

Overall, by far, the majority of respondents indicated none of these alternative risk transfer solutions were in place nor under consideration, and this matches our experience in practice. Nonetheless, it is interesting that a fairly significant number are still considering implementation in the future.

Since the survey was conducted, there has been a material development in the U.S. and in particular in Delaware, where the state has recently passed a law making it clear a standard captive, that is, a normal group company rather than a PCC or SAC, can insure directors for side A losses.

The usefulness of this law is, for now, confined to companies registered in Delaware and it remains to be seen whether any other U.S. states or indeed any other jurisdictions will adopt similar legislation.

Furthermore, while this new legislation says that non-indemnifiable claims can be paid by a captive as a matter of Delaware corporate law, it is untested in relation to claims that may be legally and practically non-indemnifiable by virtue of federal insolvency and bankruptcy laws.

It also remains unclear as to whether or not a federal court could seize the assets of the captive in a bankruptcy proceeding as an asset of the estate.

Disclaimer

Willis Towers Watson offers insurance-related services through its appropriately licensed and authorised companies in each country in which Willis Towers Watson operates. For further authorisation and regulatory details about our Willis Towers Watson legal entities, operating in your country, please refer to our Willis Towers Watson website.

It is a regulatory requirement for us to consider our local licensing requirements. The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date.

This publication offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market and we disclaimer all liability to the fullest extent permitted by law. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this video may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson.

The information given in this publication is believed to be accurate at the date of publication shown at the top of this document. This information may have subsequently changed or have been superseded and should not be relied upon to be accurate or suitable after this date. This document offers a general overview of its subject matter. It does not necessarily address every aspect of its subject or every product available in the market. It is not intended to be, and should not be, used to replace specific advice relating to individual situations and we do not offer, and this should not be seen as, legal, accounting or tax advice. If you intend to take any action or make any decision on the basis of the content of this publication you should first seek specific advice from an appropriate professional. Some of the information in this publication may be compiled from third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such. The views expressed are not necessarily those of Willis Towers Watson.

Each applicable policy of insurance must be reviewed to determine the extent, if any, of coverage for losses relating to the Ukraine crisis. Coverage may vary depending on the jurisdiction and circumstances. For global client programs it is critical to consider all local operations and how policies may or may not include coverage relating to the Ukraine crisis. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal and/or other professional advisors. Some of the information in this publication may be compiled by third-party sources we consider reliable; however, we do not guarantee and are not responsible for the accuracy of such information. We assume no duty in contract, tort or otherwise in connection with this publication and expressly disclaim, to the fullest extent permitted by law, any liability in connection with this publication. Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates. The Ukraine crisis is a rapidly evolving situation and changes are occurring frequently. Willis Towers Watson does not undertake to update the information included herein after the date of publication. Accordingly, readers should be aware that certain content may have changed since the date of this publication. Please reach out to the author or your Willis Towers Watson contact for more information.

About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success – and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW-FINEX 508810/04/22

wtwco.com