SEPTEMBER 2023

BDO's 2023 Telecommunications Risk Factor Survey

Introduction

BDO's 2023 Telecommunications Risk Factor Survey explores the risks, challenges, and opportunities facing telecoms across the globe. It charts how the industry's view of specific risks has evolved and what approaches, strategies and initiatives companies deploy to eliminate or mitigate them.

The survey examines how the telecoms industry views both its current and future state. Through its analysis, industry insiders, companies, investors, and interested parties can gain insights into what drives business decisions, investment strategies, and strategic initiatives across the telecom industry during challenging times.

CONTENTS

Methodology

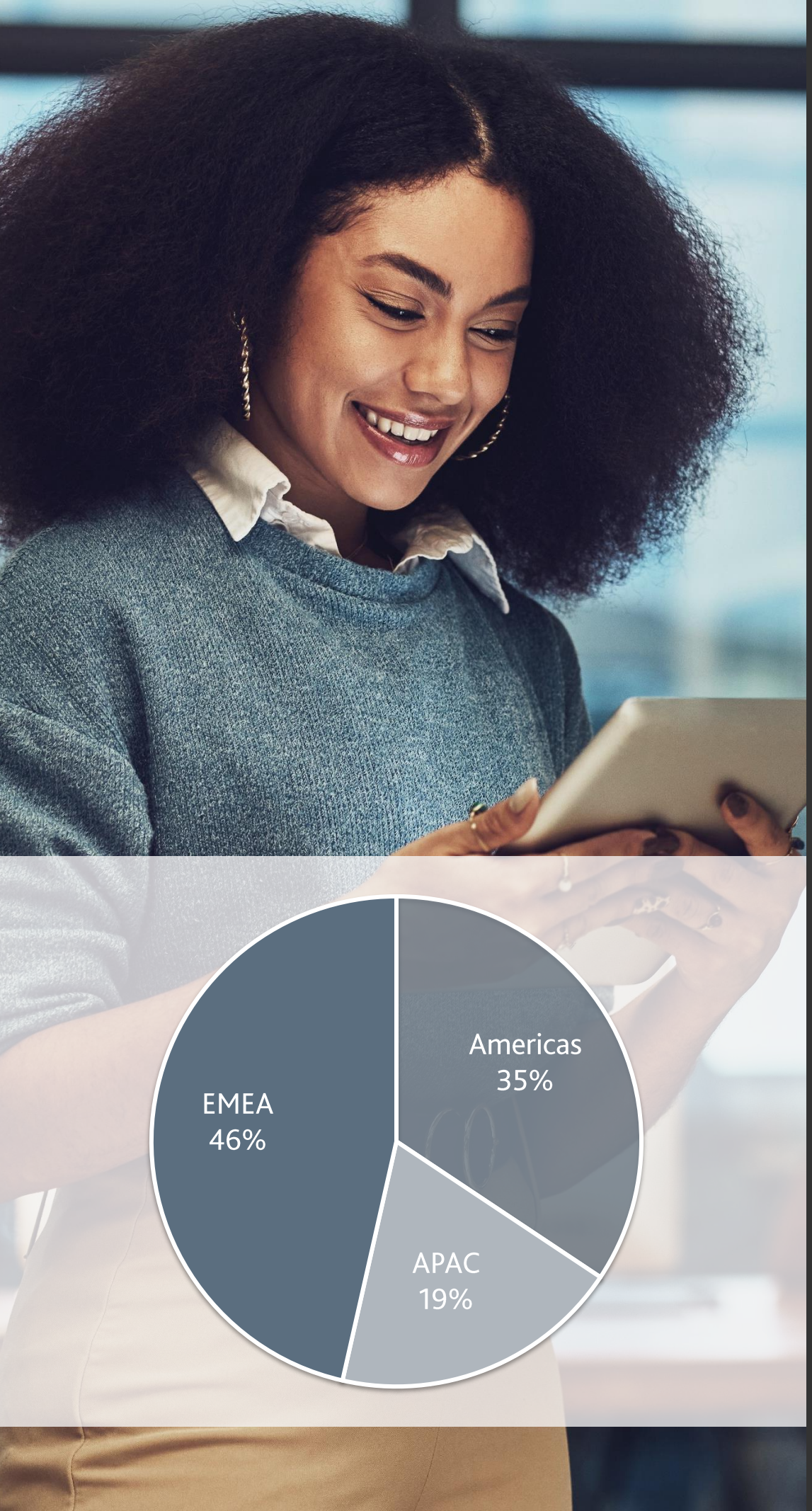
The BDO Telecommunications Risk Factor Survey identifies the most commonly reported risks for telecoms across the globe in 2022 – 2023. We used companies' annual reports as the foundation for data collection and analysis to ensure data reliability .

In this edition, we expanded our analysis to include 63 companies, compared to 49 in the previous edition.

The addition of 14 companies has influenced this year's data, resulting in an expected decrease in the overall percentage values assigned to each risk, due to the larger sample size. Consequently, our focus will be on examining how the industry's perception of specific risks has evolved, rather than emphasizing the year-on-year percentage values associated with each risk. Global and regional risks were calculated as a percentage of companies that highlighted a specific risk factor in their reports, compared to the total number of companies analysed.

As in previous editions, risks were then split into two main groups: macroeconomic risks and industry-specific risks. The top risks were identified for each group

Market coverage



46%

EMEA:

29 companies

Representation: UK (5), Germany, France, Belgium, Spain (all 3)

35%

AMERICAS:

22 companies

Representation: US (13), Brazil (4), Canada (3)

19%

APAC:

12 companies

Representation: China (3), Australia, India, Japan, South Korea (all 2)

RISK FACTORS:
7 new risk factors identified

In the 2022 edition, **46 risk factors** were collected and analyzed. This year, we uncovered an additional 7 risk factors, **totaling 53.**

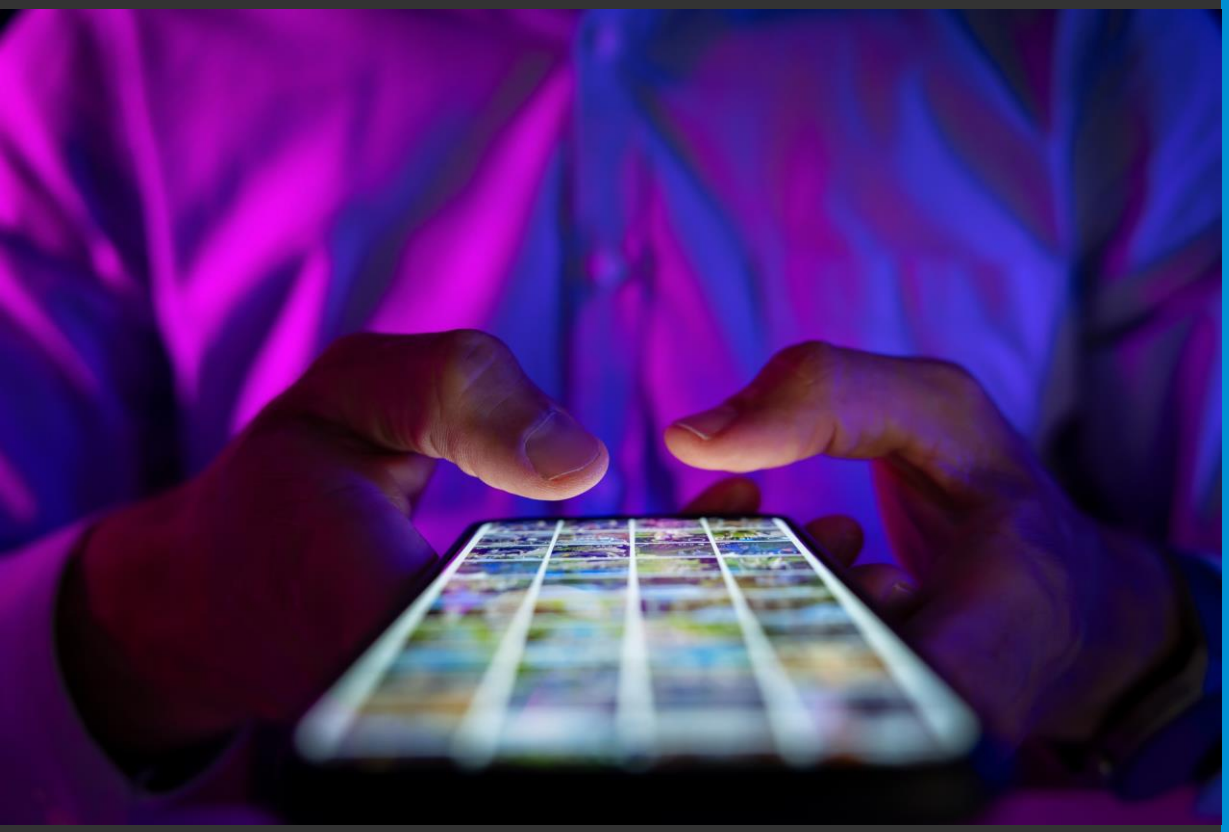
The new risk factors identified in 2023, listed in order of perceived risk (1 = most mentioned risk):

1. **COMPLIANCE ISSUES** with data privacy and confidentiality
2. **UNPLANNED DOWNTIME** causing business interruptions
3. **THREATS** to physical security and infrastructure
4. **DISRUPTIONS** from unstable supply chain conditions
5. **COMPLICATIONS** from mergers, acquisitions, and integrations
6. **SHIFTS** in customer expectations due to digital transformation
7. **CONCERNS** with leadership succession and ethical standards

As in previous editions, the 53 risks were grouped into two categories: macroeconomic and industry-specific risks. This categorisation enables a detailed assessment of risk factors based on their relevance to companies in the telecom industry.

Macroeconomic risks – **risk** factors relevant to the entire economy, or a significant portion of it, affecting businesses across industries. Also referred to as market risks or general risks.

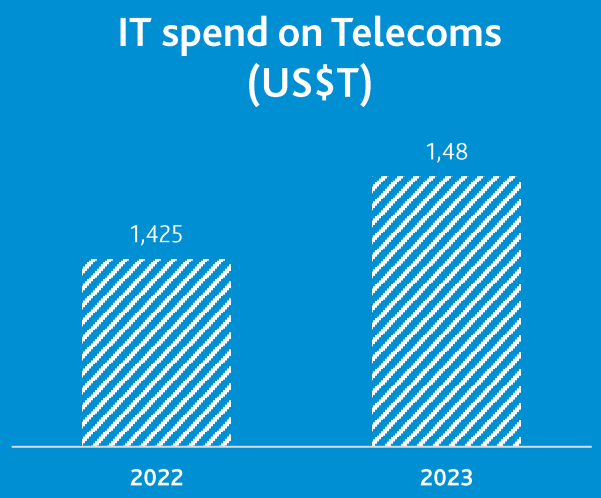
Industry-specific risks – risk factors that primarily or solely relate to the telecom industry or are especially significant to companies in the industry.



Telecoms set for continued growth in 2023

In 2023, the global telecommunications market is anticipated to experience robust growth, with an estimated worldwide expenditure of 1.5 trillion U.S. dollars. This signifies a 2.8 percent rise compared to the projected expenditure for 2022. The significance of reliable telecom services has escalated in the era of flexible, and home-working, leading organizations and governments to acknowledge the value of investing in telecom infrastructure for the digital economy .

EXTERNAL INDICATORS



"The telecoms industry is grappling with increased competition, infrastructure threats, and legislative changes, all while striving to ensure cybersecurity and address the growing concerns around climate change. It's a challenging time."

– Tom Mannion, BDO Global

EXECUTIVE SUMMARY

Navigating Turbulent Times:

Regulatory, Cybersecurity, and Climate Challenges Converge for Telecoms in 2023

BDO's 2023 Telecommunications Risk Factor Survey uncovers a complex landscape fraught with competing risk factors, from persistent regulatory and cyber-security related challenges to an increasing concern about the current and future impacts of a changing climate. As reported in BDO's Global Risk Landscape report, leaders from across sectors in 2023 grapple with the risk multiplier effect, with different risks intersecting with and amplifying one another. This risk intersectionality is certainly seen in the telecommunications sector, where a complex range of factors converges to create an uncertain environment, with pressures on profitability felt from many angles.

For leaders in telecoms, new competitors, operating on an unequal playing field, and a trend towards increased governmental overreach and new regulation are two key drivers of the complex risk landscape they face. Compounding these factors is a backdrop of a consistently volatile global economy and increasing geopolitical tensions.

In 2023, telecoms face a confluence of threatening forces – increasingly complex cyber-attacks, damage to infrastructure from extreme weather events, and innovation-stifling regulation – all of which pose unique, but equally serious risks to telecoms' core service delivery and financial security.

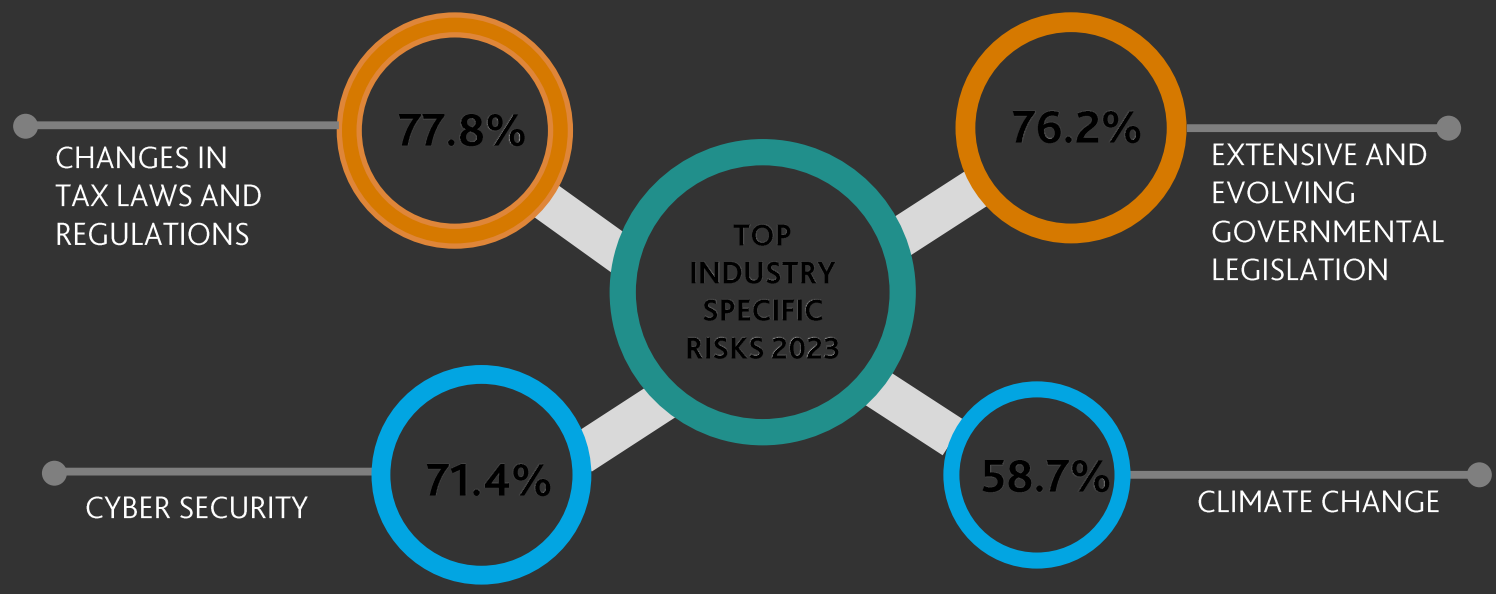
BDO Global Risk Landscape 2023, The age of the risk multiplier, July 2023, PDF, accessed - https://www.bdo.ae/en-gb/insights/global-risk-landscape-2023

INDUSTRY-SPECIFIC RISKS

The Complex Telecoms' Risk Spectrum:

Regulatory Pressures, Cyber Threats, and the Impacts of Climate Change

In 2023, the telecoms sector is confronted with a myriad of challenges that have the potential to affect firms' financial performance. Changing tax regulations is the biggest threat to telecoms, with 77.8% of companies reporting on the potential associated impacts. The increasingly complex legal and regulatory environment in which telecoms operate is putting firms under more scrutiny than ever and significantly increasing compliance costs.



Some telecoms are planning for fundamental changes to their core business models as a result of continued legislative change and persistent interventions by regulators. Most telcos are concerned by the very real threat of unsupportive regulation stifling innovation, and restricting their ability to meet core business goals, such as the rollout of 5G and fibre.

Coupled with this is an unequal regulatory playing field, where new, well-financed entrants to the market are competing with fewer regulatory burdens when compared with established telecoms. This is particularly a challenge for telecoms in the Americas, where 'Intense and increasing competition from other telecommunications services providers' ranks as the 3rd most reported risk factor.

"The complexity of the legal and regulatory environment in which we operate, and the related cost of compliance are both increasing due to additional requirements."

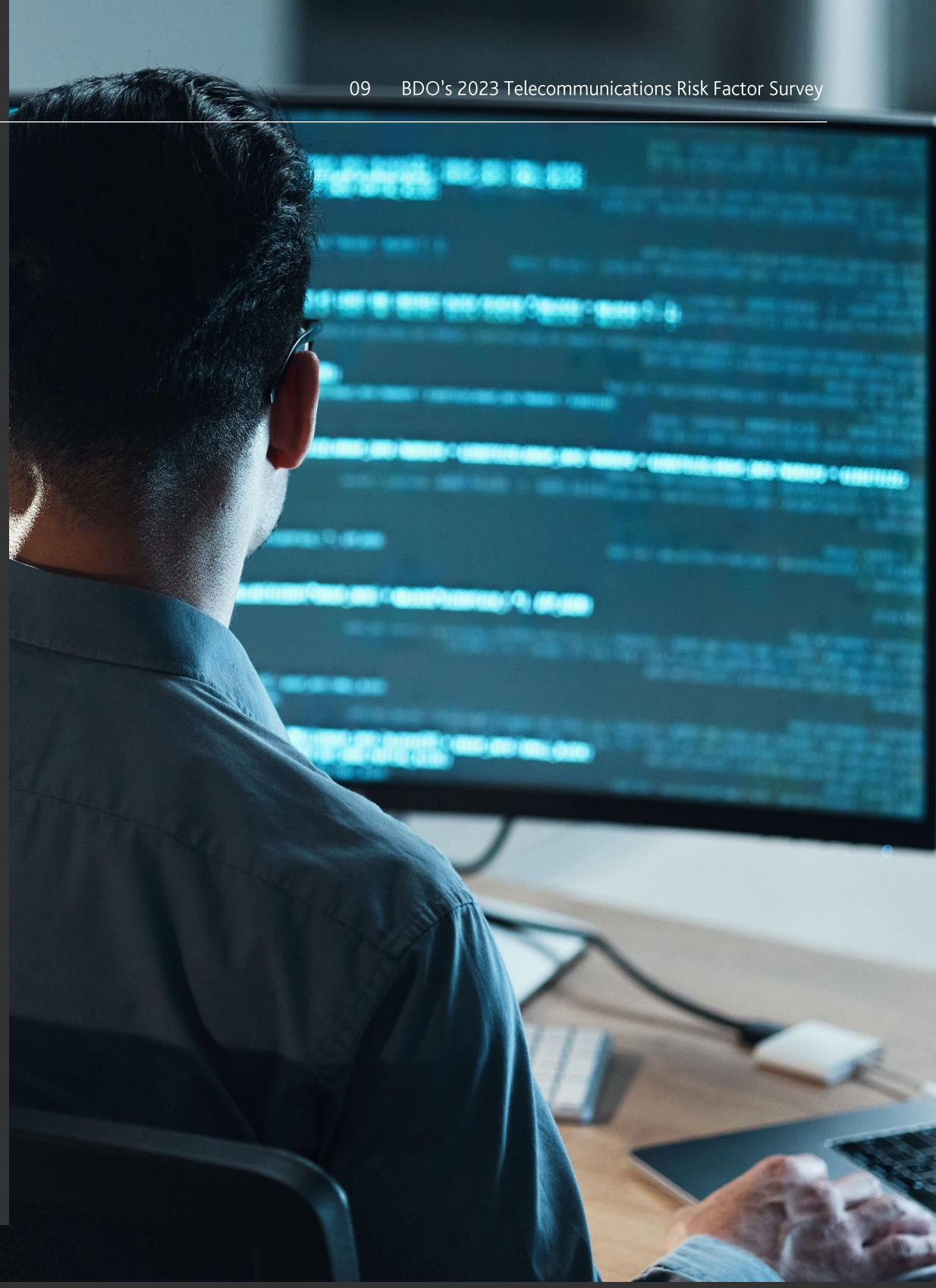
(Proximus Group, 2022)

"The industry in which we operate is highly competitive and has become more so in recent years. In some instances, we compete against companies with fewer regulatory burdens, access to better financing and greater and more favorable brand name recognition."

(Charter Communications, 2022)

Cyber threats (71.4%) are recognised as the 3rd most significant risk to the industry at a global level, with attacks increasing in both breadth and complexity.

Telecoms are particularly concerned by the impacts significant data breaches, and associated service disruptions may have on their financial performance and reputation. Poorly managed cyber events could lead to significant financial losses and reputational harm, resulting in a sustained loss of market share and greater scrutiny from regulators. Among a multitude of others, geopolitical tensions and rapid digitisation are cited as key factors driving an increase in cyber security risk in 2023. Technological developments and the increased prevalence of home working post-COVID make telecoms more susceptible than ever to cyber security risks.



"Cyber security risks have increased exponentially due to the rapid digitisation of applications and the increasing prevalence of remote working, accelerated by the COVID-19 pandemic."

(Singtel, 2022)

"In 2022, Russia's war of aggression in Ukraine also changed the security environment in Finland. Finnish organisations have faced an increased level of cyber threats, and the attacks have been more targeted than before." (Elisa Oyj, 2022)

"The transition to a low carbon economy is associated with transitional risk, e.g. policy, liability or technology risks, that may all incur additional costs." (Tele2, 2022)

Climate Change:

A New 'Top Risk' for Telecoms in 2023

Telecoms are keenly aware of the effect that the rapidly changing climate is having on their businesses (58.7%), with 'climate change risks' ranked within the top 5 risks for the first time in BDO's Telecommunications Risk Factor Survey.

Firms are concerned by the increasing frequency of extreme weather events, such as unprecedented long-term heat levels, and the damage these events cause to key infrastructure, leading to service shutdowns and significant disruption. Looking to the future, companies are also preparing for the move towards a lower-carbon global economy; a move which will come with additional costs and its own transitional risks. Investors are increasingly demanding that telecoms adopt more sustainable practices, such as increasing their levels of climate reporting. Simultaneously, telcos need to be careful to avoid accusations of greenwashing, making misleading claims about a company's environmental credentials. Such accusations can bring with them substantial reputational damage.

MACROECONOMIC RISKS

Economic Headwinds and Consistent Instability:

Telecoms Encounter Volatility, Interest Rates, Health Crises, and Political Challenges

57.1%	Foreign exchange risk (fluctuations in exchange rates)
=	
57.1%	Political instability in operating markets
52.4%	Interest rate risk (significant fluctuations in the fair value of financial instruments)
50.8%	Public health crises, including the COVID-19 pandemic and resulting mitigation measures
=	
50.8%	Unfavourable economic conditions, such as recession or economic slowdown
46%	Failure to meet the evolving environmental, social, and governance (ESG) practices or benchmarks
41.3%	Adverse changes in the global financial markets (inability to access capital needed to fund business operations)

Top macroeconomic risks 2023

From a macroeconomic perspective, our research shows that telecoms are most concerned by threats associated with continued global economic volatility ('Foreign exchange risk' – 57.1%, 'Interest rate risk' – 52.4%, 'Unfavourable economic conditions' – 50.8%).

Telecoms transacting in multiple currencies are vulnerable to exchange rate volatility, caused by fiscal and political factors beyond their control. Exposure to significant changes in exchange rates impacts cash flows and overall equity, with companies using hedging instruments to manage their foreign currency exposure on expenditures and operational costs.

Firms report particular concern over rising interest rates and resultant increased borrowing costs, which lead to higher debt burdens and reduced profitability. Looking more widely, persistently unfavourable economic conditions, characterised by plateaus and increases in inflation, erode the purchasing power of consumers, potentially resulting in reduced demand for telecommunication services and products. Telecommunications companies forecast a struggle to maintain profitability amidst higher operating costs and a possible slowdown in customer acquisition.

"The telecoms industry is grappling with increased competition, infrastructure threats, and legislative changes, all while striving to ensure cybersecurity and address the growing concerns around climate change. It's a challenging time."

– Tom Mannion, BDO Global

"We are exposed to fluctuations in currency values, changes in relationships between U.S. and foreign governments, war or other hostilities, and other regulations that materially affect our earnings."

– (AT&T, 2022)

Three years on from the start of the COVID-19 pandemic, telecoms are still planning for the threats associated with delivering core services amid public health crises (50.8%), however, the concern has unsurprisingly fallen drastically since our previous survey (83.7%). Now, telecoms are focusing on limiting disruption associated with health crises, by increasing operational resilience and preparedness.

Telecoms continue to be affected by political instability in operating markets (ranked joint 1st, 57.1%). The continued war in Ukraine has led to a decline in financial markets and has fuelled inflationary increases globally, as well as presenting significant operational challenges for companies in neighbouring nations. Multi-national telecoms directly experience the effect of a global economy that is more interconnected than ever, whilst also being extremely volatile, with existing geo-economic orders being questioned and reconfigured. [5]

5. Tyson, L & Zysman, J, Berkeley Roundtable on the International Economy (BRIE), "Preparing for a Volatile Global Economy," working paper 2023-01, accessed July 3, 2023, https://brie.berkeley.edu/sites/default/files/publications/brie_working_paper_2023-01_preparing_for_a_volatile_global_economy.pdf.

MACROECONOMIC RISKS

SHIFTING RISK DYNAMICS:

Climate Change Risks Emerge as a Key Consideration for Telecoms in 2023, alongside Persistent Cyber Security Risk and Continued Changes to Laws and Regulations

Top-5 global risks 2023

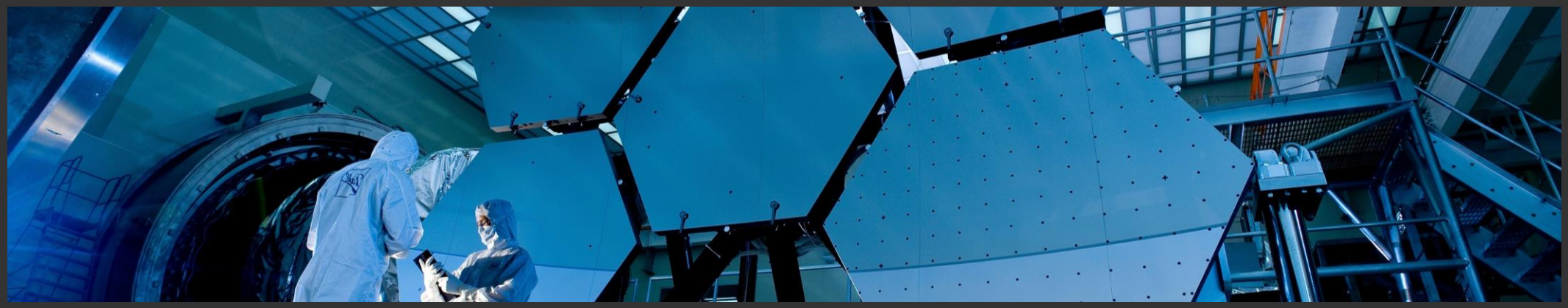
1. Changes in tax laws and regulations — 77.8%
2. Extensive and evolving governmental legislation — 76.2%
3. Cyber security — 71.4%
4. Climate change — 58.7%
5. Foreign exchange risk — 57.1%

Top-5 global risks 2022

1. Interest rate — 98%
2. Extensive and evolving governmental legislation — 91.8%
3. Credit risk — 89.8%
4. Intense and increasing competition — 89.8%
5. Cyber security — 89.8%

In 2022, telecom companies underwent transformative changes, adapting to increasing connectivity demands from individuals and businesses.

The telecom market landscape continued to evolve due to technological developments and changing customer preferences. To stay competitive amidst these challenges, companies fortified their internal processes, revised their investment strategies, and improved their service offerings.
The rapidly changing industry necessitated a robust risk management framework. In the previous edition, the top 5 risks faced by these companies were analysed in depth.



Risks associated with interest rates, foreign exchange, credit, intense market competition, and regulatory changes were among the most significant. The capital-intensive nature of the industry, heightened by COVID-19, posed market risks like interest rate, foreign currency, credit, and liquidity risks. Additionally, companies faced industry-specific risks including regulatory changes, competition from peers and other industries, cyberattacks, security breaches, technological disruptions, inadequate IT infrastructure, and an inability to respond to technological advancements and introduce competitive products.

However, by 2023, the focus of risks has notably pivoted. Changes in tax laws and regulations, along with extensive and evolving governmental legislation, have become increasingly significant risk factors. Furthermore, environmental issues, especially concerns related to climate change, have also emerged as key areas of focus. This change in the risk landscape shows a clear shift from purely financial and market-related risks towards more legislative, environmental, and still prevalent cybersecurity risks, emphasising the dynamic and multifaceted nature of risk factors within the industry. The industry now finds itself grappling with increased competition, infrastructure threats, and legislative changes, all while striving to ensure cybersecurity and address the growing concerns around climate change.

"Governments are looking to protect jobs and protect national security interests."

– Tom Mannion, BDO Global

"Our towers are subject to physical climate-related risks associated with natural disasters (including as a result of any potential effects of climate change) such as tornadoes, fires, hurricanes, floods, and earthquakes or may collapse for any number of reasons, including structural deficiencies."

(SBA Communications, 2022)

The shift towards climate change as a significant risk factor in the telecommunication industry is in part driven by a growing awareness of the associated threats posed, as well as heightening regulatory pressures from governments. In the past, the impact of environmental factors on industries was often overlooked. However, recent years have seen a dramatic increase in the recognition of how industries contribute to climate change and are in turn affected by it.

Climate change has a significant impact on telecommunications infrastructure. Extreme weather events exacerbated by climate change, such as hurricanes, floods, and wildfires, can damage physical infrastructure, leading to service disruptions and substantial costs. Additionally, higher temperatures strain the cooling systems of data centres, increasing operational costs and energy consumption, hence affecting the profitability of telecom companies. Whilst wrestling with these physical threats in the current, in 2023, many telcos are sharing ambitious decarbonisation strategic and financial aims for the near future, aiming to significantly reduce their carbon footprints. In practice, companies are taking steps such as the phasing out of petrol and diesel vehicles, to be replaced with electric vehicles. Implementing such actions will incur substantial costs in the short and medium term for telcos.

REGIONAL MARKET ANALYSIS

In the following segmentation analysis, we explore the risk factors that differentiate each of the three markets from the global risk landscape for telecoms in 2023.

AMERICAS

81.8 %

Changes in tax laws and regulations

68.2 %

Lawsuits, claims or other legal proceedings

Extensive governmental legislation

63.6 %

Intense and increasing competition

Foreign exchange risk

APAC

75 %

Cyber-attacks

Changes in tax laws and regulations

Extensive governmental legislation

Interest rate risk

66.7 %

Climate change

Compliance issues with data privacy

58.3 %

Intense and increasing competition

Foreign exchange risk

50 %*

Public health crises

EMEA

82.8 %

Extensive governemtnal legislation

79.3 %

Cyber-attacks

75.9 %

Changes in tax laws and regulations

65.5 %

Unplanned downtime causing business interruptions

*capped risks at 50% minimum for market analysis, to ensure reported data is meaningful.

RISK WATCH: AMERICAS

Intensifying Competition, Legal Battles, Political Uncertainty & Rate Volatility

In the Americas, along with mounting pressure and scrutiny from changes in tax laws and regulations, the industry is facing significantly heightened competition (the 3rd most frequently mentioned risk in the region). Emerging satellite start-up companies are seeking to disrupt the market with new, more affordable options. This increased competition has the potential to reduce market share for existing players, which may lead to price wars in an already highly commoditised market. In addition, these new companies benefit from a less heavily regulated environment, in comparison with telecoms, who must deal with increased costs from noncompliance to ever-changing regulations.

"We face significant competition from other service providers, as well as other well-capitalized entrants in the video and data services industry, which could reduce our market share and lower our profits." *(Cable One, 2022)*

Lawsuits, claims, or other significant legal proceedings also present a considerable threat to the stability and profitability of telecom companies in the Americas. Telecoms commonly become embroiled in numerous legal claims surfacing from a range of areas such as consumer protection breaches, non-compliance with existing or new regulation, or infringement of intellectual property rights.

Whilst many lawsuits may not seem material or immediate, the outcome of such proceedings can lead to high costs, such as the tarnishing of a well-established brand reputation, and distracting management's focus from core business operations. Furthermore, regulatory proceedings related to internet wholesale costing and pricing can potentially affect a telecoms business significantly. Lawsuits resulting in substantial litigation costs, awards, or settlements could negatively affect the company's bottom line and raise concerns among stakeholders. Lastly, non-compliance with evolving data privacy regulations such as California's Consumer Privacy Act could lead to fines, awards of damages to litigants, or decreased revenue, thereby further destabilising the telecoms firms.

"If the Company is convicted in judicial or administrative proceedings, the results of its operations and its financial condition could be adversely and significantly affected." *(Oi S.A., 2022)*

Political instability in operating markets presents a significant challenge to the performance and growth of telecom companies in the Americas. Telecoms often operate in multiple countries within the market, where they must abide by a broad range of complex local laws, regulations, and treaties. Changes in these laws or regulations can create an unpredictable operating environment, potentially affecting the ability to manage and expand their businesses as intended.

RISK WATCH: AMERICAS

Intensifying Competition, Legal Battles, Political Uncertainty & Rate Volatility (continued)

"We have international operations, particularly in Mexico, and other countries worldwide where we need to comply with a wide variety of complex local laws, regulations and treaties." *(AT&T, 2022)*

Given the significant role it plays in the global telecom industry, the impacts of negative economic conditions or overarching political decisions in the U.S. would reverberate globally, destabilising telecom operations not only domestically but also in international markets. Telecom companies may be forced to limit or cease operations, terminate customer relationships, or abandon lucrative opportunities in countries that become subject to sanctions or other business restrictions imposed by governments. This risk underscores the need for such companies to monitor not only the local political climate in the markets where they operate but also international geopolitical developments that could indirectly influence their operations.

"We may be required to limit or halt operations, terminate customer or client relationships or forgo profitable opportunities in countries which may, in the future, be subject to sanctions or other restrictions on the business activity of corporations such as TELUS, by U.S. or Canadian legislation, executive order or otherwise." *(Telus, 2022)*

Foreign exchange fluctuations also pose a considerable threat to the financial stability of telecom companies operating in the Americas. As many telecoms have international operations and are likely to expand into new markets, they are exposed to foreign exchange risk. Telecom companies hedging US dollar-denominated expenditures could be adversely affected if the US dollar significantly depreciates. Similarly, currency devaluation in a specific country or region could impact the financial results of telecom businesses operating in those markets. Changes in foreign currency rates relative to the U.S. dollar, therefore, could have either positive or negative implications for their operating results.

"Changes in foreign currency rates relative to the U.S. dollar could positively or negatively impact our operating results." *(Lumen, 2022)*

RISK WATCH: ASIA-PACIFIC (APAC)

Interest Rate Vulnerability, Data Privacy Compliance, and Cybersecurity Challenges

Telecoms in APAC navigate an extremely complex risk landscape. As well as facing the cyber security, and regulatory challenges recognised by firms on a global level, telcos in APAC are particularly concerned by the impacts of rising interest rates. Telecoms holding debts issued at floating interest rates are exposed to cash flow interest rate risk, while those issued at fixed rates are exposed to fair value interest rate risk. This hinders telecoms' ability to innovate and invest in fundamental infrastructure upgrades in the region.

"Debts carrying interest at variable rates and at fixed rates expose the Group to cash flow interest rate risk and fair value interest rate risk, respectively."
(China Telecom, 2022)

Firms in APAC also report a high level of concern regarding compliance with data privacy. Telcos must comply with far-reaching laws recently introduced in the region, such as the Data Security Law, and Personal Information Protection Law of the People's Republic of China, both established in 2021 . Additionally, companies recognise how working with third parties increases the likelihood of unexpected information security compromises.

"Even though we strive to take all steps we believe are necessary to protect personal information, hardware, software or applications we develop or procure from third parties may contain defects or other problems that could unexpectedly compromise information security."
(KT, 2022)

As cyber-attacks continue to increase in both complexity and magnitude, telecoms in APAC are acutely aware of the need to build greater resilience within their core IT infrastructure. Firms are taking active steps to deepen data security and risk screening, putting systems in place which empower their employees and customers to avoid errors which lead to breaches.

"The Company will deepen data security and user personal information protection, accelerate the use of data and intelligence injection for the security core platform, continue to carry out network security risks screening, effectively ensure reliable operation of network security as well as data and personal information security."
(China Telecom, 2022)

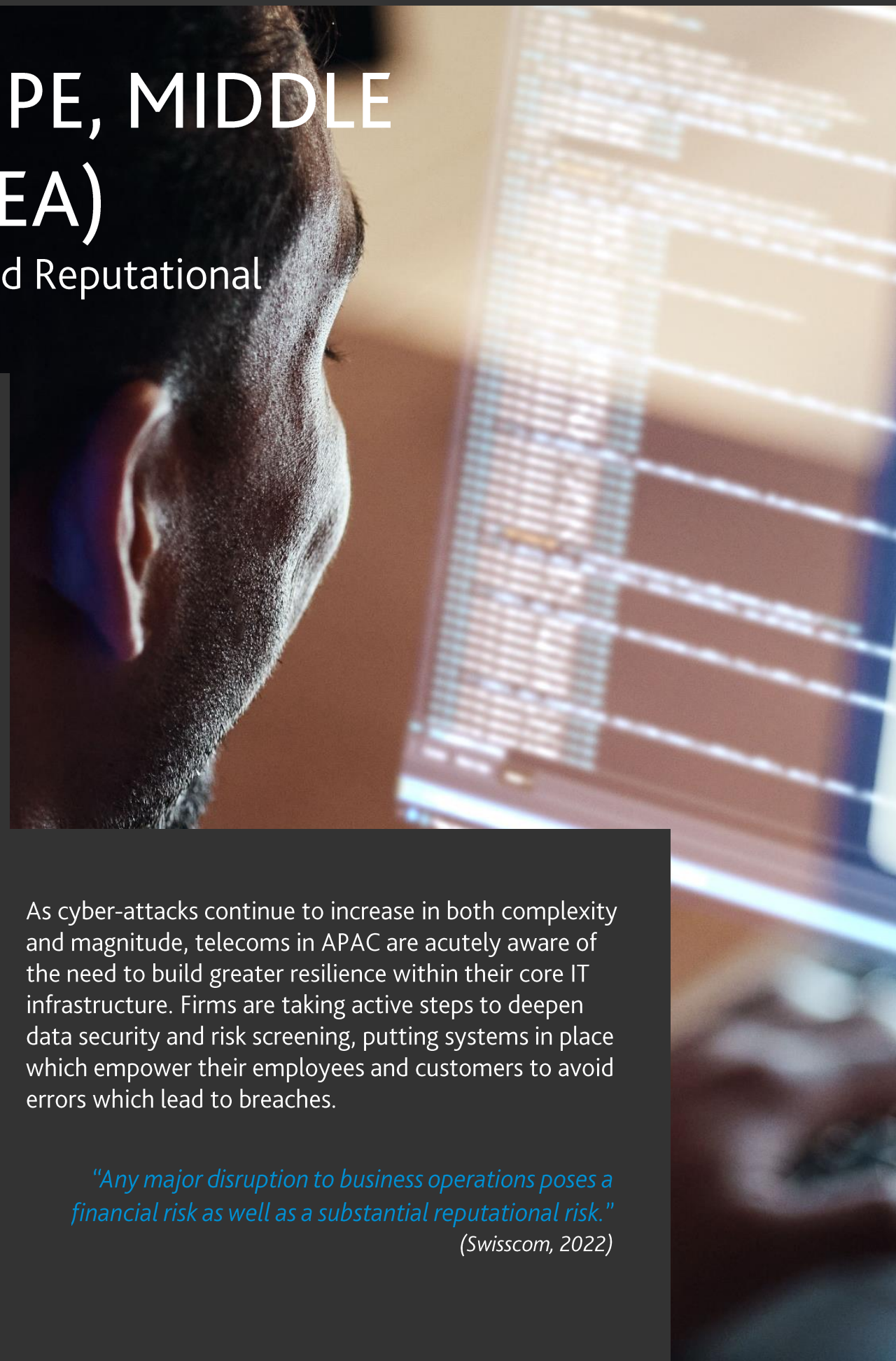
RISK WATCH: EUROPE, MIDDLE EAST & AFRICA (EMEA)

Cyber-Attacks, Connectivity Issues, and Reputational Damage Concerns

In EMEA, Telecoms are particularly focused on the risks posed by cyber-attacks. Being heavily reliant on external vendors for infrastructure, products, and services to complement and enhance their own, means that telcos are in a particularly vulnerable position. Third party service providers are often a source of security defects for telecoms in the region, which in practice can incur substantial costs if IT infrastructure is breached..

"Actual or perceived security breaches or attacks on our systems or those of our third-party service providers may cause us to incur increasing costs."
(Freshworks, 2022)

Such breaches often lead to disruptions, including an interruption of core services. Interruptive events carry substantial reputational risk for telecoms and emerge as the 5th most frequently cited risk for firms in EMEA. As rapid digitisation continues, connectivity between differing systems becomes a more pressing challenge for telcos. Connectivity issues can lead to technical malfunctions, resulting in an interruption. Telecoms in the region also report on the interruptive challenges associated with transferring customers from old to current service platforms. As well as causing interruptions in service for those customers being transferred, there is a considerable risk of customer churn and loss during these events.



As cyber-attacks continue to increase in both complexity and magnitude, telecoms in APAC are acutely aware of the need to build greater resilience within their core IT infrastructure. Firms are taking active steps to deepen data security and risk screening, putting systems in place which empower their employees and customers to avoid errors which lead to breaches.

"Any major disruption to business operations poses a financial risk as well as a substantial reputational risk."
(Swisscom, 2022)

RISK MITIGATION:

How are Telecoms Responding to Today's Risks?

In 2023, telecommunication companies across the globe have dedicated teams and structures in place to plan for, mitigate and respond to risks effectively. Typically, telcos have a Risk Management Team, chaired by a leadership team member, responsible for identifying and evaluating macro-risk factors. These teams work in collaboration with a range of others, such as Compliance, Internal Audit, and Business Continuity teams to address and tackle risks when they emerge. Below we've collated some of the more common mitigation strategies leveraged by Telcos in the face of the risks emerging in 2023.

RISK TYPE	2023 SIGNIFICANCE	CHARACTERISTICS	MITIGATION STRATEGIES
Regulatory risks	Account for 3 of the Top 5 risks for Telecoms in 2023 (changes in tax laws, new regulation, extensive government legislation)	Non- compliance New and changing regulations. International requirements	Monitor – engage in ongoing regulatory analysis, 'horizon scanning' for changes and evaluating how they may impact operations. Connect – maintain close relationships with regulatory authorities and policymakers to anticipate legislative changes. Develop – employee experts through training, so they know where legal and compliance risks come from, and how to get expert help to handle them. Examine – carry out assurance on day-to-day operations, regions, partners, projects, and suppliers. Investigate anomalies and remedy these proactively.
Cyber-security risks	The 2nd most cited risk for Telecoms in 2023. A particular concern for telcos in APAC and EMEA	Data breaches Supply chain & third-party vulnerabilities Reputational damage	Vigilance – detect external threats and respond to cyber risks before they become incidents. Gather intelligence on evolving cyber techniques, tactics, and capabilities. 'Hygiene' – promote good security behaviour among colleagues through training, communications, and campaigns. Develop a prevention and maintenance mindset, in which employees are 'cyber savvy'. Team – establish a Chief Information Security Officer responsible for leading enterprise-wide information security strategy, policy, standards, architecture, and processes. Global scale – implement a global information security management program including administrative, technical, and physical safeguards, periodically engaging with both internal and external auditors and consultants to assess and enhance the program.
Climate change risks	In the Top 5 risks for the first time at a global level	Damage to infrastructure Energy transition Energy demands	A 'Green' Vision – formulate a "Green Innovation toward 2040" environment and energy vision and advance initiatives to reduce environmental impact to achieve carbon neutrality by 2040. Align – with recommendations from the Task Force on Climate-Related Financial Disclosures (TCFD). Use the TCFD's referenced scenarios to review climate-related risks around transitioning to a lower-carbon economy. Upgrade – invest in physical defences and upgrades at affected sites. For instance, construct flood defences, and install cooling system upgrades.

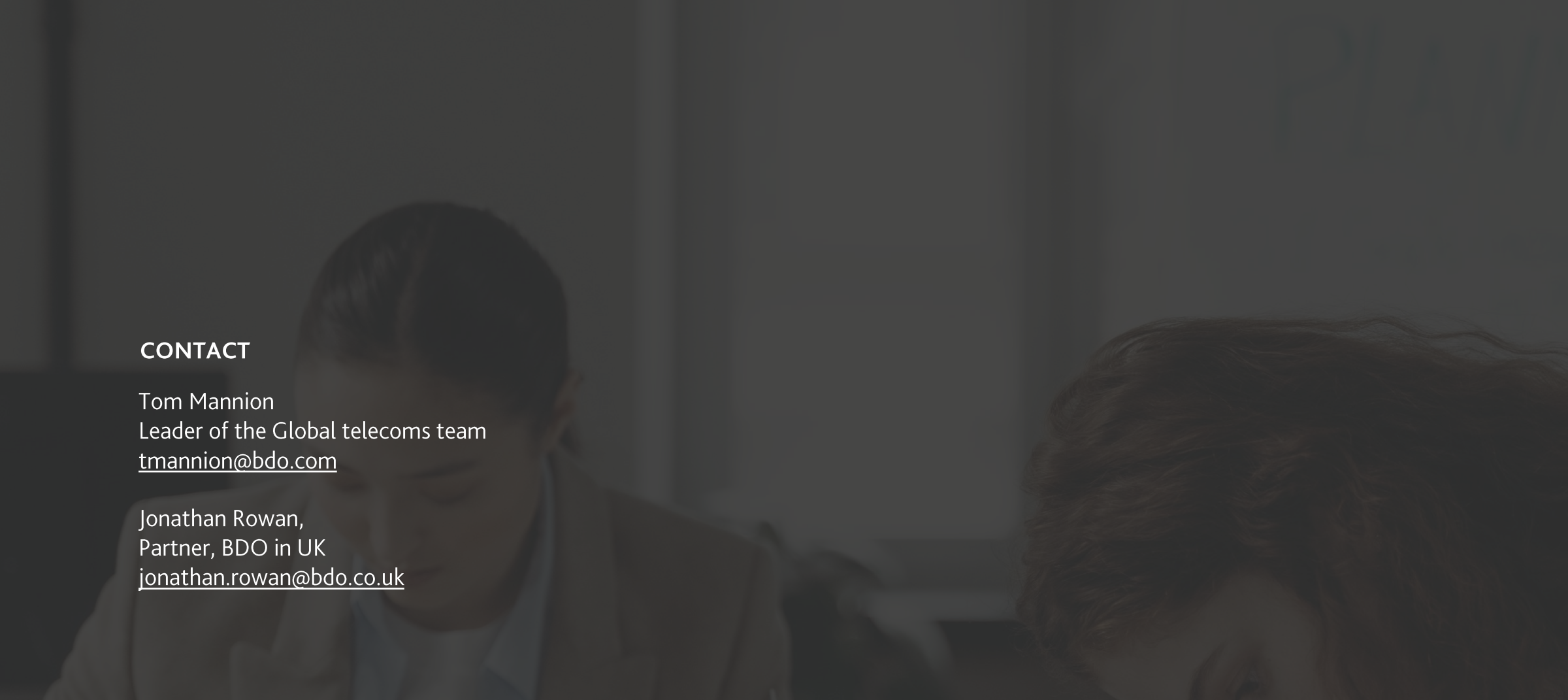
[1] BT Group plc, Annual Report 2022, p. 61, 'Legal compliance'
[2] Ibid., p., 60
[3] Ibid., p.61
[4] Ibid., p.62
[5] Nippon Telegraph and Telephone Corporation, Annual Report 2022, pp., 56 – 57, 'Reinforcing Security'
[6] BCE INC. Annual Financial Report 2022, p.27, 'How information security governance helps create value'
[7] Verizon, 2023 Proxy Statement, p. 16, 'Oversight of ESG strategy and risks'
[8] Lumen, 2022 Annual Report | 2023 Proxy Statement, p., 43, 'Risk Oversight'
[9] Nippon Telegraph and Telephone Corporation, Annual Report 2022, p., 53, 'Risk Management'
[10] Lumen, 2022 Annual Report | 2023 Proxy Statement, p., 48, 'Sustainability Initiatives'
[11] BT Group plc, Annual Report 2022, p. 67, 'Climate change strategy'
[12] Ibid, p., 67

REFERENCES

- BDO, Global Risk Landscape 2023, The age of the risk multiplier, July 2023, PDF, accessed - https://www.bdo.ae/en-gb/insights/global-risk-landscape-2023
- Tyson, L & Zysman, J, Berkeley Roundtable on the International Economy (BRIE), "Preparing for a Volatile Global Economy," working paper 2023-01, accessed July 3, 2023, https://brie.berkeley.edu/sites/default/files/publications/brie_working_paper_2023-01_preparing_for_a_volatile_global_economy.pdf.
- Website: Statista, "Telecommunications Market - Statistics & Facts," accessed July 3, 2023, https://www.statista.com/markets/418/topic/481/telecommunications/#statistic2.
- Website: Forbes, "Keeping Up with International Data Privacy Regulations," Forbes Tech Council, July 5, 2023, accessed July 5, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/07/05/keeping-up-with-international-data-privacy-regulations/
- Website: California Attorney General's Office, "Consumer Privacy FAQs: California Consumer Privacy Act (CCPA)," accessed July 5, 2023, https://www.oag.ca.gov/privacy/ccpa

REFERENCES: COMPANY REPORTS CITED IN REPORT TEXT (in order of mention)

- Proximus Group, (2022), Integrated Annual Report 2022 (p. 306) - https://www.proximus.com/dam/jcr:29b8b936-587f-4624-825d-051276d8e4c2/proximus-integrated-annual-report-2022_en.pdf
- Charter Communications, (2022), Reimagining Connectivity, 2022 Annual Report (p.19) - https://www.annualreports.com/HostedData/AnnualReports/PDF/OTC_CHTR_2022.pdf
- Singtel (Singapore Telecommunications Limited), (2022), Annual Report 2022 (p. 77) - https://www.optus.com.au/content/dam/optus/documents/about-us/media-centre/annual-reports/2022/Singtel-Annual-Report-2022.pdf
- Elisa Oyj (Elisa Corporation), (2022), Annual Review, 2022 (p. 11) - https://www.annualreports.com/HostedData/AnnualReports/PDF/elisa-oyj_2022.pdf
- Tele2, (2022), Annual and Sustainability Report 2022 (p. 29) - https://www.tele2.com/files/Main/3372/3745977/tele2-annual-and-sustainability-report-2022.pdf
- Du, (Emirates Integrated Telecommunications Company PJSC), (2022), Annual Report 2022 (p.35) – [accessed via] https://www.du.ae/about-us/investor-relations/disclosures-and-reports
- AT&T Inc., (2022), 2022 Annual Report (p. 28) - https://investors.att.com/~/media/Files/A/ATT-IR-V2/financial-reports/annual-reports/2022/2022-complete-annual-report.pdf
- SBA Communications Corporation, (2022), 2022 Annual Report, (p. 17) - https://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_SBAC_2022.pdf
- Cable One, (2022), Annual Report 2022, (p. 27) - https://s25.q4cdn.com/936561952/files/doc_financials/2021/ar/2022-Annual-Report.pdf
- OI S.A, (2022), Annual Report 2022, (p. 35) - https://api.mziq.com/mzfilemanager/v2/d/6aebbd40-9373-4b5a-8461-9839bd41cbbb/a8a18de5-c588-5a26-80e5-546of310dd24?origin=1
- Telus, (2022), 2022 Annual Report, (p. 125) - https://assets.ctfassets.net/fltupc9ltp8m/3kd6XgcS6RcRS7Iv86xnka/5600bbfa2d03ae8397ec9391dd7f4c0c/TELUS-2022-annual-report_acc_03312023.pdf
- Lumen, (2022), 2022 Annual Report, 2023 Proxy Statement, (p. B-23) - https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_LUMN_2022.pdf
- China Telecom Corporation Limited, (2022), Annual Report, 2022, (pp. 55 – 271) - https://www.annualreports.com/HostedData/AnnualReports/PDF/NYSE_CHA_2022.pdf
- KT Corporation, (2022), 2022 Annual Report, (p. 9) – [accessed] https://corp.kt.com/eng/
- Freshworks Inc., (2022), Annual Report 2022 (p. 23) – https://stocklight.com/stocks/us/services/nasdaq-frsh/freshworks/annual-reports/nasdaq-frsh-2022-10K-22664720.pdf
- Swisscom Ltd., (2022), Annual Report 2022 (p. 59) - https://reports.swisscom.ch/download/2022/en/swisscom_geschaeftsbericht_gesamt_2022_en.pdf



CONTACT

Tom Mannion
Leader of the Global telecoms team
tmannion@bdo.com

Jonathan Rowan,
Partner, BDO in UK
jonathan.rowan@bdo.co.uk

www.bdo.global