RESILIENCE BAROMETER 2020

Build resilience. **Protect** value.

EXPERTS WITH IMPACT

FTI CONSULTING

Contents

Introduction

Companies across the G20 are facing increasingly complex risks arising from technology transformation, geopolitical tensions and the polarisation of the political landscape. As businesses confront cybersecurity threats, fight financial crime and prepare for more changes in legislation and regulation in 2020, our survey reveals that many executives remain unprepared for a new wave of risks and crises.

Upcoming elections in the United States, Brexit and the increase in cyber attacks and regulatory actions, globally, are just a few examples of the complexities driving new threats. Our survey found that failure to fully understand and prepare for the impact of external threats could decrease revenue by as much as five percent, highlighting the imperative of resilience for businesses today.

Encouragingly, in the face of such a dramatic increase in risk, this year's survey did point to a small improvement in resilience scores, suggesting that some organisations are managing to contain and manage emerging threats through better preparedness. 84% of business leaders surveyed were anticipating a crisis in 2020, with many stepping up their adoption of new technologies. Artificial intelligence, blockchain and machine learning are playing a particularly significant role both in transforming business models and combating global financial crime and cyber attacks.

Around the world, FTI Consulting professionals work closely with clients to anticipate and address the increasingly complex business challenges arising from the risks featured in this report. By testing the impact of 18 distinct scenarios most likely to negatively impact the bottom line, adversely affect reputation and lead to increased regulatory pressure, companies can develop strategic responses to today's emerging threats.

An additional challenge facing today's executives is the need to build personal resilience in response to new levels of threat and disruption. Such resilience underpins businesses' continued ability to thrive, as they face increased pressure to grow turnover, strengthen their brands, as well as engage with regulators and activist consumers.

We would like to thank the extensive network of senior business leaders who have contributed to this project, taking the time to provide their invaluable perspectives with regard to the most pressing challenges facing businesses in 2020 and beyond.

We welcome your feedback.

STEVEN H. GUNBY
President and Chief Executive Officer

KEVIN HEWITT
Chairman, EMEA region

Executive **Summary**

The FTI Consulting Resilience Barometer 2020 shows that in the face of emerging threats, most companies across the G20 remain unprepared. This lack of resilience detracts from their ability to take advantage of opportunities and invest for future growth.

RESILIENCE SCORE 2020 **43**

Measured out of a total score of 100, the FTI Consulting resilience score gauges how well companies are prepared to deal with both internal and external corporate risks most likely to negatively impact their turnover, value and reputation.

The score is based on the incidence and actual impact which 18 scenarios have on turnover – as well as how proactively corporate leaders believe they are managing those risks. In this way, the Resilience Barometer captures both the impact and likelihood of failures of resilience on their organisations.

Our latest research finds that large companies across G20 countries slightly improved their average resilience score from 40 to 43 over the past year, showing some improvement in the proactive management of these corporate risks.

The low overall score, however, suggests there is much more companies can do to effectively prevent and manage company risks.

"The 2020 elections in the United States, the looming UK exit from the EU, cyber attacks and increasing regulatory actions are just a few examples of challenges we see companies grappling with each day. It is not a matter of if a company will face an inflection point or crisis, but when it will happen — meaning the senior executives and businesses that are most prepared are likely to remain the most resilient, competitive and viable."

KEVIN HEWITT
Kevin Hewitt, Chairman, EMEA region

RESILIENCE SCORE 2020 BY COUNTRY AND INDUSTRY

Country	Score	Change to G20 average
INDIA	60	17
BRAZIL	58	15
INDONESIA	54	11
CHINA	51	8
MEXICO	47	4
CANADA	47	4
SOUTH AFRICA	46	3
TURKEY	45	3
ITALY	44	1
US	43	<1
FRANCE	40	-3
JAPAN	40	-3
AUSTRALIA	39	-4
UK	36	-7
RUSSIA	36	-7
ARGENTINA	35	-8
SOUTH KOREA	35	-8
SAUDI ARABIA	33	-10
GERMANY	32	-11

G20 43

Industry	Score	Change to G20 average
RESOURCE TRANSFORMATION (INDUSTRIALS AND CHEMICALS)	49	6
CONSUMER GOODS	48	6
TECHNOLOGY & COMMUNICATIONS	46	3
FOOD & BEVERAGE	44	1
FINANCIALS	43	<1
INFRASTRUCTURE	42	-1
RENEWABLE RESOURCES & ALTERNATIVE ENERGY	38	-5
SERVICES	37	-6
TRANSPORTATION	36	-7
EXTRACTIVES & MINERALS PROCESSING	36	-7
HEALTHCARE	35	-8

2,276

LARGE COMPANIES

C-suite and senior manager perspectives from 2,276 large companies across G20 countries.

$44 trillion

GLOBAL TURNOVER

Participating companies represent a sum aggregated global turnover of USD$44 trillion.

58 million

PEOPLE EMPLOYED

58 million people are directly employed by the companies researched.

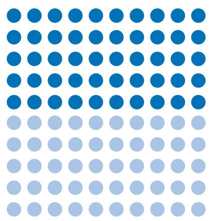
Executive **Summary**

Seven of the countries with above-average resilience are in emerging markets.

CORPORATE RISKS - PREPARING FOR EMERGING THREATS

50%

of the companies we surveyed use Artificial Intelligence or Machine Learning to help avoid or prepare for emerging threats.



'LEAKS OF SENSITIVE INTERNAL COMMUNICATIONS' CLIMBED INTO THE TOP FIVE CORPORATE RISKS FROM SIXTH POSITION LAST YEAR.

READ MORE ON PAGE 8

CRISIS - THE HIDDEN COST

87%

of respondents claim they have had a significant crisis situation **negatively impacting their business in 2019.**

84%

of companies surveyed expect a crisis in 2020.

36%

reported mental health issues as a result of dealing with a crisis.

READ MORE ON PAGE 12

REGULATION - DIALOGUE TO CREATE SUSTAINABLE FRAMEWORKS

81% +5%

of respondents expect to see an increase in regulations in the next 12 months, compared to 76% last year.

71%

of large companies have been investigated for market dominance in the last 12 months.

42%

of leaders believe they should personally comment on political and regulatory changes affecting their company.

READ MORE ON PAGE 14

FINANCIAL CRIME - MOVING BEYOND DATA SILOS

64%

of respondents have been exposed to a financial crime over the last 12 months.

40% REPUTATIONAL DAMAGE

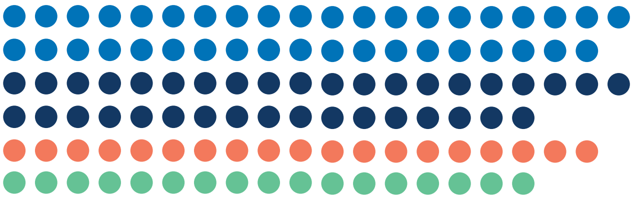
44% LOST REVENUE

Of those that suffered a financial crime, lost revenue and reputation damage were the top two negative consequences in 2019, with 44% of senior executives reporting lost revenue and 40% reputational damage.

FINANCIAL SERVICES COMPANIES CONTINUE TO FACE INTENSE SCRUTINY, WITH **67% OF RESPONDENTS HAVING HAD AN INVESTIGATION ON FINANCIAL PRACTICES** IN THE LAST 12 MONTHS.

READ MORE ON PAGE 18

SUSTAINABILITY - ENGAGING FOR GROWTH



39%

of respondents say the biggest pressure to be more transparent comes from regulators, compared to **37% for customers**, **19% for media** and **13% from activists or NGOs**.

THE TOP FIVE REPORTED ISSUES ARE:

1. Energy consumption **65%**
2. Employee health and safety **60%**
3. Labour practices **54%**
4. Anticorruption practices **53%**
5. Management of the legal and regulatory environment **52%**

READ MORE ON PAGE 22

CYBERSECURITY - RESILIANCE REQUIRES PROACTIVITY

OF G20 LEADERS SURVEYED BELIEVE THEY HAVE CYBERSECURITY GAPS.

At least 1 in 4 organisations surveyed have experienced a cyber attack where assets were stolen or compromised in the last 12 months.

20%

of companies were victims of a ransom or data hostage situation in 2019.

28%

of respondents believe 'employee awareness, security, culture and training' are their biggest security gaps, and 35% have invested in this area over the past 12 months.

READ MORE ON PAGE 26

TECHNOLOGY - TRANSFORMING BUSINESS MODELS

59%

OF RESPONDENTS BELIEVE AI & MACHINE LEARNING WILL IMPACT SIGNIFICANTLY OVER THE NEXT 10 YEARS

READ MORE ON PAGE 28

Corporate Risks: Preparing for emerging threats

Companies across the globe are facing unprecedented and increasingly complex challenges as digital disruption accelerates structural, geopolitical and societal changes. As these global risks intensify, companies need to rethink their preparedness strategies to build resilience.

A key element in measuring a company's resilience is assessing both the likelihood and the impact of potential corporate risks on the bottom line as well as their level of preparedness to counter such risks.

Our research shows that company leaders across the globe acknowledge that the increasing number and severity of unforeseen events will demand more involvement from the board in the future, with 79% of respondents agreeing that boards should play a proactive role in anticipating potential risks.

While risks such as fraud, litigation and corruption and political disruption still rank highly on the concerns of business leaders, it is clear that cyber-related risks are escalating to become the foremost threat.

Yet despite the profound role that technological disruption has had in shaping the risk landscape for companies, the vast majority remain unprepared in the face of these increased risks.

Triggered by increasing digital dependency and the integration of technology into all facets of business and society, our survey shows that cyber attacks stealing or compromising assets remain by far the biggest threat facing companies, with 27% of respondents having experienced such an incident in the past 12 months.

Major product defects also rank amongst the top five corporate risks, with 24% of business leaders having experienced an incident over the past 12 months compared to 21% in 2019. Changes in regulations, disrupted supply chains, social media driving increased consumer awareness and malicious cyber attacks are just some of the emerging reasons for a rise in product recalls.

There was also a strong correlation between those respondents who felt under 'extreme' pressure to increase turnover and those reporting major product defects over the past 12 months – 38% reporting product defects in this category, far higher than the 24% G20 average.

In this year's survey 'Leaks of sensitive internal communications' climbed to the third highest corporate risk from sixth position last year. Over the past 12 months, 21% of companies experienced some form of significant data breaches. While 57% of respondents report that they are 'mainly proactive' when it comes to managing major corporate risks, such as product defects, only 45% manage the threat of cyber attacks and leaking of sensitive internal communications proactively. This is despite the likelihood and large impact of cyber attacks on lost turnover.

Trade restrictions as a result of rising geopolitical tensions and changing power balances between the world's most powerful nations is a top concern for business leaders in 2020. More than one fifth of respondents experienced trade restrictions over the past 12 months and are expecting this trend to continue.

In an increasingly interconnected and global world, companies accustomed to dominant positions in protected markets continue to face increasing competition from new entrants as well as regulatory pressure.

"There is a thin line between the desire to communicate with external audiences around a crisis and having enough robust information to disseminate. Demonstrating command of a situation through well-considered, active communications can help protect the brand, valuation and reputation of companies and ensure business continuity."

NEIL DOYLE
Senior Managing Director, Strategic Communications

Of particular interest to shareholders and investors is the correlation between companies put under 'extreme' pressure to increase revenue and the incidence of corporate risks experienced. Across almost every corporate risk category, when companies are required to meet extreme revenue goals, it has a negative impact on their resilience compared to companies not facing similar pressure. In an attempt to overcome hurdles, business leaders may be tempted to short cut R&D, for example, make riskier decisions and forgo investment in preventative risk management tools resulting in less protection against corporate risks that could potentially have a significant impact on their revenues.

In a world of finite business resources, balance is key and building resilience is often a case of either/or, rather than doing everything. In response to corporate risks, 50% of G20 companies say they use artificial intelligence and analytics to detect threats and trends, up from 47% of the previous year. Tools such as conducting market research to understand stakeholder perceptions are also widely used, while conducting crisis simulations is another popular approach taken by companies in their efforts to prepare for corporate risks.

TOP FIVE CORPORATE RISKS FOR 2020

1	Cyber attacks stealing or compromising assets
2	Major product defect
3	Leak of sensitive internal communications
4	Trade restrictions
5	Litigated against

"In an interconnected world, companies face more than the usual commercial risks when they invest across jurisdictions. The dramatic growth of international arbitration as a mechanism for dispute resolution is an indication that both investors and governments are willing to invest resources to protect their value and reputation."

JOHN ELLISON
Senior Managing Director, Economic and Financial Consulting

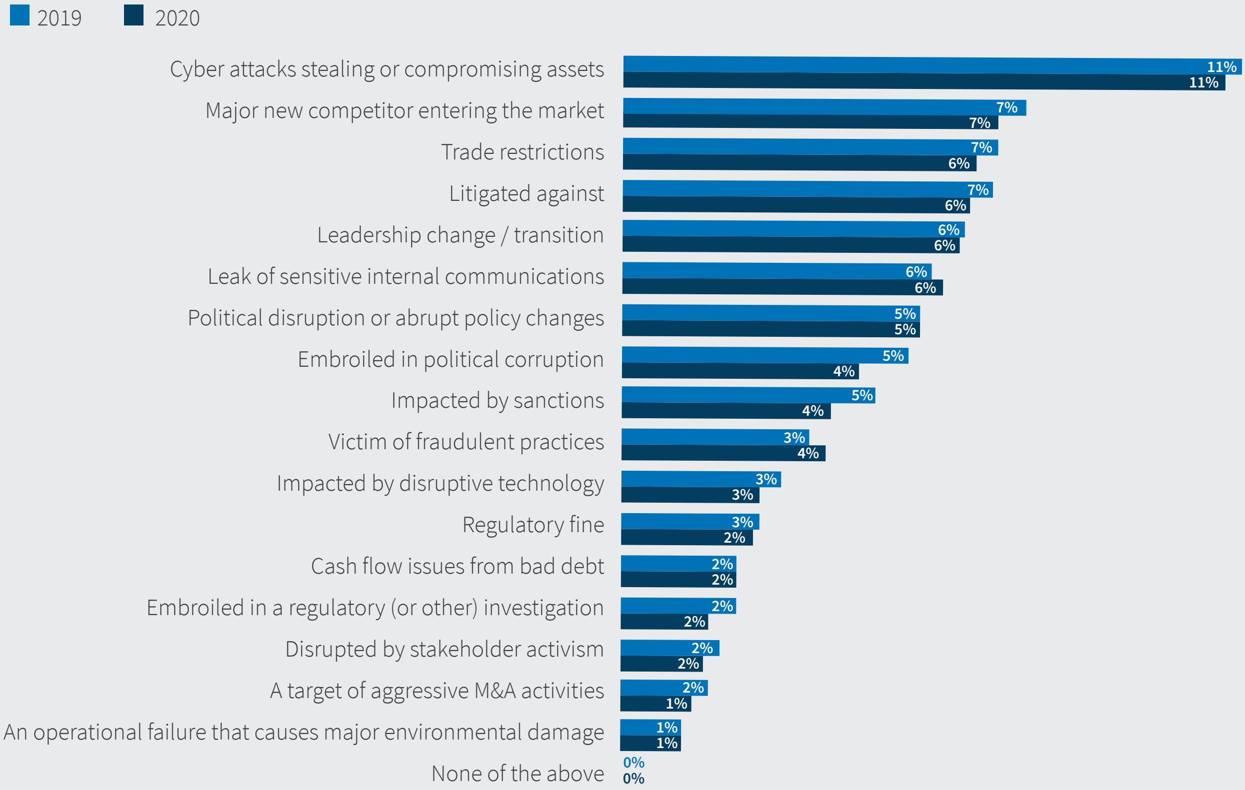
RISK SCENARIOS EXPERIENCED

Q. Which of the following are you aware of happening to your company over the last 12 months?

Cyber attacks stealing or compromising assets	27%	-3 ▼
Major product defect	24%	+3 ▲
Leak of sensitive internal communications	21%	+1 ▲
Trade restrictions	20%	-1 ▼
Major new competitor entering the market	20%	-1 ▼
Litigated against	20%	-2 ▼
Leadership change / transition	20%	-1 ▼
Political disruption or abrupt policy changes	19%	=
Impacted by sanctions	15%	-2 ▼
Embroiled in political corruption	15%	-2 ▼
Victim of fraudulent practices	15%	=
Impacted by disruptive technology	11%	-1 ▼
Embroiled in a regulatory (or other) investigation	11%	=
Disrupted by stakeholder activism	11%	=
Regulatory fine	11%	-2 ▼
A target of aggressive M&A activities	8%	-1 ▼
An operational failure that causes major environmental damage	8%	=
Cash flow issues from bad debt	8%	-1 ▼
None of the above	17%	+3 ▲

IMPACT ON TURNOVER

Q. Out of these events, what proportion would you say each has had an impact on your lost turnover?



ACTIONS TO HELP PREPARE FOR SCENARIOS THAT IMPACT TURNOVER

Q. Which of the following does your company do to help avoid or prepare for such situations?

50% +3 ▲
Use AI and analytics to detect threats and trends

44% -1 ▼
Conduct market research to understand stakeholder perception

38% -3 ▼
Conduct crisis simulations

35% -7 ▼
Screening of suppliers/clients/other parties

33% -5 ▼
Pre-screening of applicants before hiring

32%
Cyber-preparedness audit*

29% -9 ▼
Conduct other audits/reviews (such as internal audit)

28% =
Conduct regularly specific fraud detection procedures

25% -3 ▼
Implement an anonymous reporting system for employees

25%
Engagement with stakeholders/investors*

24%
Drive and implement cultural change*

** Not asked in previous year*

84%

OF COMPANIES SURVEYED EXPECT A CRISIS IN 2020

"When a company is less resilient, discretionary capital ends up being used to reactively protect the business and remedy reputational harm, rather than for proactively improving performance. Setbacks don't just harm the results for the last quarter or for the past year, they lessen a company's ability to invest for the future."

ALEX DEANE
Senior Managing Director, Head of UK Public Affairs, Strategic Communications

Crisis: The hidden cost

Our survey shows that the financial and reputational health of a company is not the only measure affected when a crisis hits. It also shows the damaging effects crises can wreak on the psychological and physical health of senior executives tasked with steering the company through challenging times.

While being unprepared for corporate risks can impact negatively on a company's turnover, there is often an unseen effect on the senior managers and leaders. Respondents across the board report that being unprepared for dealing with crisis takes a toll on the health and well-being of senior managers and executives.

We know from neuroscience that moments of high stress can affect performance. At a time when we rely on our leaders to make the right decisions, and quickly, they need personal resilience to make those decisions effectively.

More than a third of business executives report negative mental health issues, such as stress, worry, panic attacks, anxiety and depression as a consequence of time spent thinking about or actually dealing with crisis situations. A further 34% report interrupted sleep and physical health issues such as exhaustion and burnout.

In the fast-paced world of the modern crisis, it seems that not enough time is given to protecting those who are in charge of making the right decisions.

We underestimate the impact that a crisis can have on the physical health of those caught in the eye of the storm.

Crises tend to be all consuming while they last and it's interesting to note the impact that this is having not only on the mind, but on the body as a whole as the methods we rely on to keep well during peace time – exercise, hobbies, relaxation – get pushed to one side. Striking also was the impact that respondents pointed to in relation to their relationships. Almost one in five say a crisis has

"The growth of social media combined with increased activism from all stakeholders and a culture of antagonism towards corporates has the potential to escalate the velocity of a crisis. Companies need to invest in preparing their leaders to be crisis-ready with the same rigour and discipline as they do in helping the organisation to achieve readiness."

JAMES MELVILLE-ROSS
Senior Managing Director, Strategic Communications

had a detrimental impact on their relationships with their colleagues, which is understandable. Perhaps less obviously, 20% of business leaders also report that crises take their toll on their relationships at home. Longer working hours and work distractions when at home, leading to a lack of attention to the needs of family, are the likely culprits.

Overall, 90% of respondents claim they have had a crisis situation over the last 12 months and 87% claim there has been some negative impact.

This research suggests that companies are not preparing leaders sufficiently to manage a crisis. There needs to be recognition that the resilience of an individual depends on their wellbeing – and that business managers who are not prepared to deal with high stress situations are unlikely to prove resilient when the pressure is on. Examples of best practice captured in this survey include programmes inviting senior executives to take part in crisis simulations to ensure their personal readiness to deal with such situations and to identify gaps where further support needs to be provided.

A culture of resilience is often characterised by low power-distance ratios - enabling junior employees to engage with or challenge people who are senior to them as well as enabling senior staff members to engage with, consult or listen to people in their teams.

Leaders most likely to be resilient in the face of difficult business challenges are those most likely to be the best prepared. As a crisis unfolds and evolves, companies need to provide their senior executives with regular access to new data and information to help inform their tactics and strategy. They also need to consider the types of support provided in terms of gathering evidence to help executives conduct a diagnosis, develop solutions, appraise options and move onto effective execution in a crisis situation.

"Given that 36% of respondents have suffered mental health issues as a result of dealing with a crisis, the importance of personal resilience and for leaders to be equipped physically and mentally to deal with a fast moving situation is a business imperative. Part of that preparation is having access to the data to make informed decisions under pressure and in real time."

SIMON LEWIS
Vice Chairman in EMEA
Global Head of Financial Services
Strategic Communications

TAKING A TOLL

Q. As a consequence of the time spent thinking about or actually dealing with crisis situations over the last 12 months, what has been the negative impact upon you personally?

36%
Mental health issues (stress, worry, panic attacks, anxiety, depression)

34%
Physical health issues (exhaustion, burnout, poor diet)

34%
Interrupted sleep

29%
Interruption to your day job

20%
Deterioration in relationships with your spouse and family

19%
Deterioration in relationships with your colleagues

4% Other

13% There was no negative impact

10% I have not had a crisis situation

Regulation: Dialogue to create sustainable frameworks

Technology transformation, geopolitical tensions and polarisation of the political landscape has made for more complex regulatory risks facing companies today. Resilient companies are engaging with a range of stakeholders in the policy-making process, re-affirming their licence to operate.

Our research shows that 81% of respondents expect to see an increase in regulations in 2020, compared to 76% last year.

Businesses face not only the spectre of increased regulations in their local markets, but as regulators collaborate across borders and develop common aims in certain sectors such as Big Tech or Financial Services, it has led to a convergence of regulatory standards in certain industries which can impact operations on a global scale.

On the other hand, some jurisdictions continue to adopt more protectionist and nationalist stances in their oversight roles, leading to fragmentation in regulation across different markets.

"Businesses that factor in and engage in proactive, constructive dialogue to build sustainable regulatory frameworks that are inclusive of all constituents' interests and objectives are better able to protect their freedom to operate and create value."

JULIA HARRISON
Senior Managing Director, Global Head of Public Affairs & Government Relations, Strategic Communications

Two areas of increased regulatory focus include those governing Big Tech and companies' use of data, as well as those related to Environmental, Social and Governance issues as the political and economic spheres become more closely intertwined. Respondents also highlighted the following areas for increased regulation in 2020: market dominance (71%); financial practices (67%); products/services (66%); and compliance (65%).

The type of regulatory action taken differs from market to market, with India, China and Mexico having the highest percentage of investigations into market dominance in 2019, with India leading the way at 91%. India has also experienced the Competition Commission of India (CCI) investigating multiple cases in the last 12 months.

Our research also shows that business leaders believe the power balance between companies and regulators is shifting, with 82% of respondents rating the potential of governments and politicians to impact the performance of their business or strategic direction of their organisation, second only to customers at 88%. The Financial industry at 53% is the highest in rating 'Government/Politicians' as having a very strong potential to impact, while the Services sector is lowest at 29%.

In this context, business leaders are recognising that they need to play a more active role in the policy making process - today 39% of respondents feel they should actively engage regulators to help with the development of or changes to regulations. In fact, given the impact of regulations, 81% of leaders believe they should personally comment on political and regulatory changes affecting their company.

"To cope with the volume and complexity of regulations, firms are investing in technology to speed up compliance implementation and monitoring. More advanced firms also proactively scan the horizon for future regulatory risks that could have a major impact on their organisation, providing visibility to the compliance function to make appropriate adjustments."

STELLA MENDES

Senior Managing Director, Co-Leader of Financial Services, Forensic & Litigation Consulting

Despite the increasing influence of regulators on businesses, alarmingly, 72% of respondents felt that they still needed to improve regulatory safeguards, indicating that a significant percentage of corporates do not believe that they have achieved a satisfactory level of resilience in this key area.

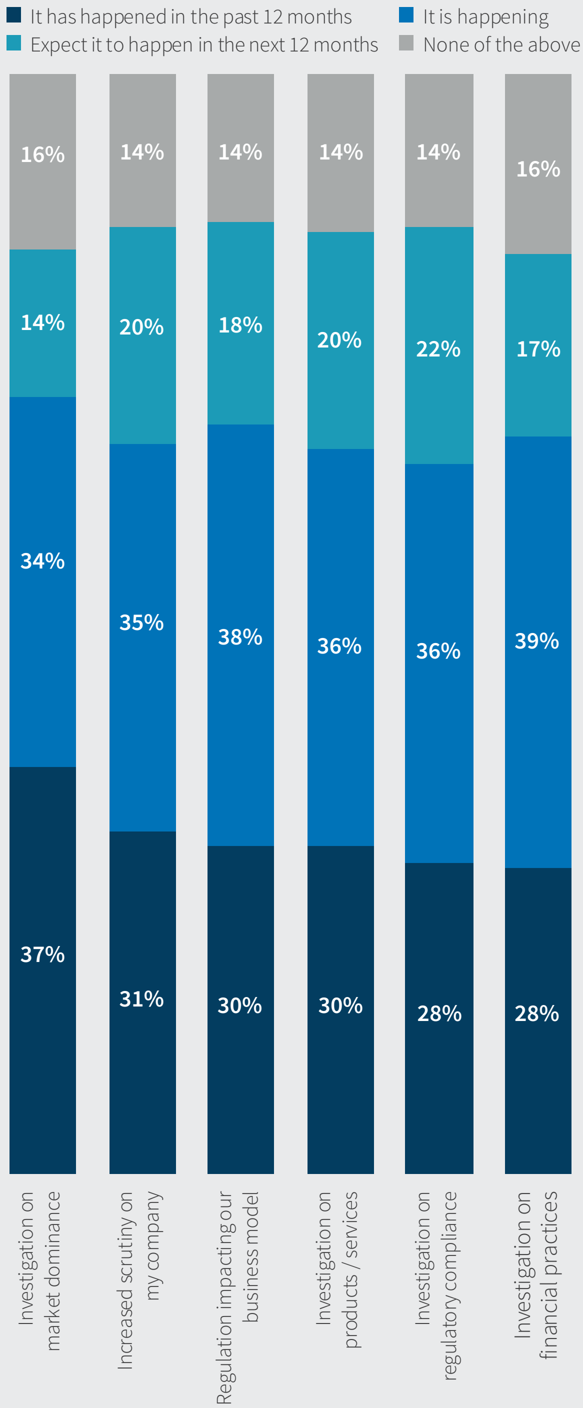
This lack of resilience reflects the number of companies currently being investigated by regulators - 67% of all G20 respondents. In addition, 11% of respondents admitted to having been fined by regulators in the past 12 months, a trend set to increase in the upcoming year.

In response to regulatory change, 43% of companies are considering adapting internally to develop competitive advantage, with 50% of companies in the Transportation sector. Meanwhile one in four said they would restrict investment and 32% said they would reduce the number of employees based in the country. Others focus on changing financial or legal structures to reduce the impact of regulation.

When businesses engage in the regulatory conversation through dialogue not only with politicians and regulators, but with a range of stakeholders, they can help build more sustainable policy frameworks. The upside of this proactive approach is greater policy consistency and predictability - key concerns for businesses across the globe.

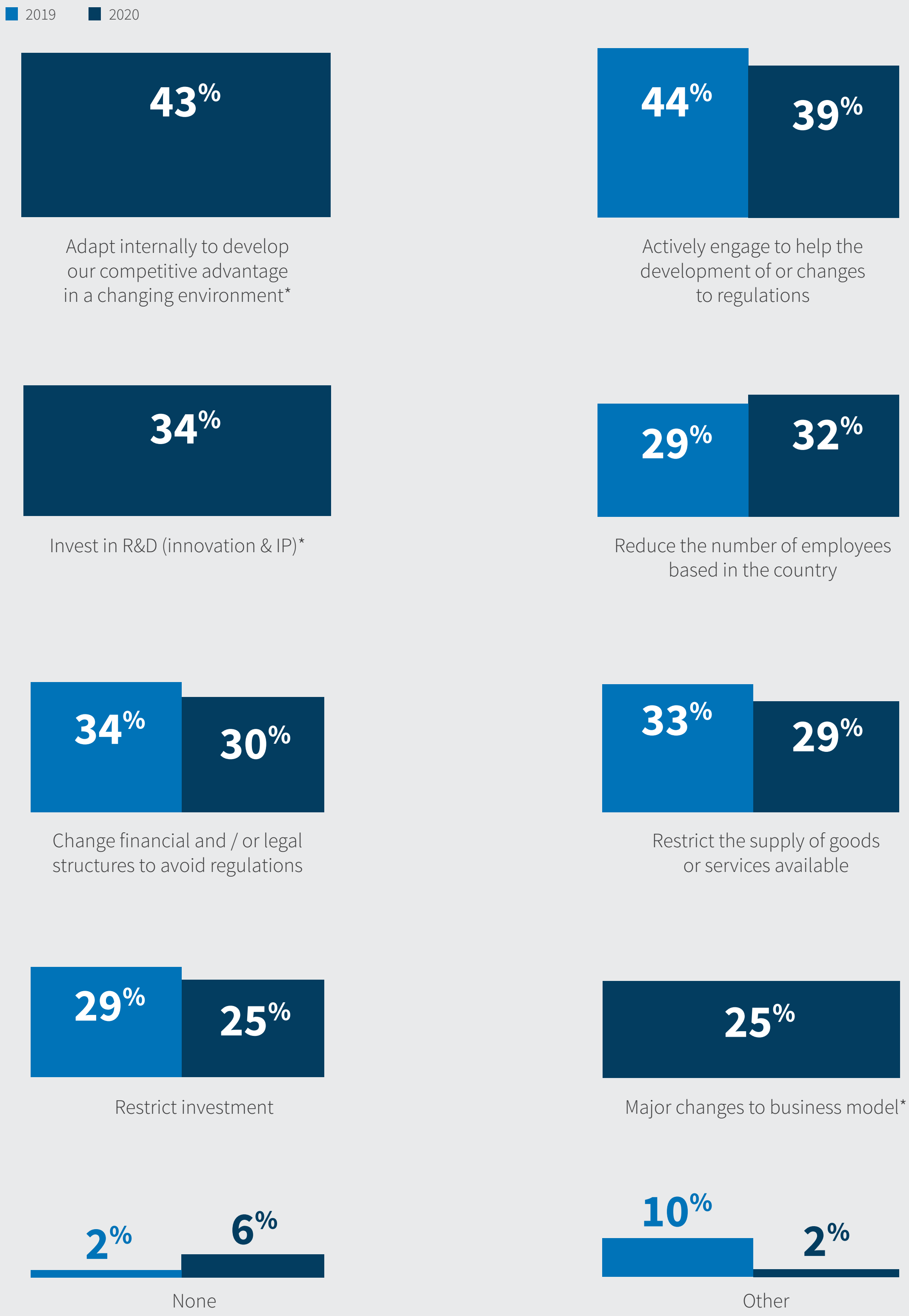
REGULATORY INVESTIGATIONS

Q. Which of the following has or are you expecting to happen to your company in your country



COMPANY ACTIONS AS A RESULT OF REGULATORY CHANGES

Q. What is your company seriously considering as a direct result of present or expected regulatory changes?



* *Not asked in previous year

50%

OF RESPONDENTS USE AI TO HELP AVOID OR PREPARE FOR CRISIS SITUATIONS

"By their very nature, data-driven technologies can destroy or redefine old boundaries. Building resilience requires new weapons to assess vulnerabilities, protect data across ecosystems and fight against financial crime. Over half of the companies we surveyed already use Artificial Intelligence and Machine Learning to help avoid or prepare for emerging threats. We all have a stake in how these outcomes will impact the global economy, public trust and the future shape of society."

CAROLINE DAS-MONFRAIS
Senior Managing Director
Chief Strategy Officer, EMEA

ftiresiliencebarometer.com
#ResilienceBarometer

Financial Crime: Moving beyond data silos

New technologies are driving increasingly sophisticated financial crimes. Threats such as fraud, bribery, corruption, money laundering and terrorist financing are gaining momentum, challenging companies' resilience in a digitally-driven era.

Our survey shows that 64% of companies were exposed to financial crime over the past year, negatively impacting revenues and causing companies' long-term reputational damage.

In the last 12 months, 15% of G20 companies have been the victim of fraudulent practices; impacted by sanctions or embroiled in political corruption, while 11% report being part of a regulatory (or other) investigation. Of the financial crimes assessed, fraud had the highest incidence at 28%.

As in our previous survey, theft and fraud represent the largest category of financial crime in 2020, with both having an incidence of 24% over the previous 12 months. Around one in five have also been affected by bribery and corruption, insider trading and money laundering.

Moreover, not only did 44% of senior executives report lost revenue as a negative consequence of financial crime, but 40% said it caused reputational damage to their firms. Other consequences included lost customers; employees leaving; management attention diverted; loss of stock market value; being litigated against; regulatory fines; and new hires deciding not to join.

It is surprising then that our findings show that around 90% of respondents believe they are fully prepared to deal with fraud, up 3% from 2019, with 83% agreeing they have a

"To combat financial crime we need accountable, transparent and collaborative institutions. Businesses play an important role in creating a cleaner global financial system by more accurately assessing and addressing security risks, improving transparency and working with regulators to develop global solutions to tackle financial crime."

ANDREW PIMLOTT

Senior Managing Director, Forensic & Litigation Consulting structured fraud response plan. However, only 42% claim they are mainly proactive at managing fraud.

Financial Services companies continue to face intense scrutiny, with 67% of respondents having experienced an investigation into financial practices in the last 12 months or currently being investigated.

Fraud continues to be the number one financial crime anticipated in 2020: 28% of respondents expect to be actively or inadvertently affected by it. This is closely followed by bribery & corruption (26%), theft (26%), insider trading (25%), money laundering (22%) and tax evasion (22%).

Leveraging technology is a crucial tool in helping to detect and protect companies against financial crime. Respondents say they are increasingly using artificial intelligence and data analytics as tools for risk avoidance, with 50% claiming they are using it to prepare for/avoid risk – up 3% from last year.

Crisis simulations, screening of suppliers/applications and internal audits have decreased since 2019. Only 28% regularly conduct specific fraud detection procedures - the same percentage as last year.

22%

INCREASE IN COMPLIANCE SPEND TO COMBAT GROWING THREATS EXPECTED IN 2020

In addition, 83% say they are proactively engaging with regulators and governments on this issue.

Cybersecurity and preventing financial crime go hand in hand: 46% of respondents use cybersecurity to manage financial crime risk, followed by staff training and compliance, fraud detection procedures and advanced analytic detection. The least reported methods include ‘Know Your Customer’ onboarding and period checks, as well as due diligence on third parties.

Astoundingly, 5% of organisations do not have any anti-financial crime procedures in place.

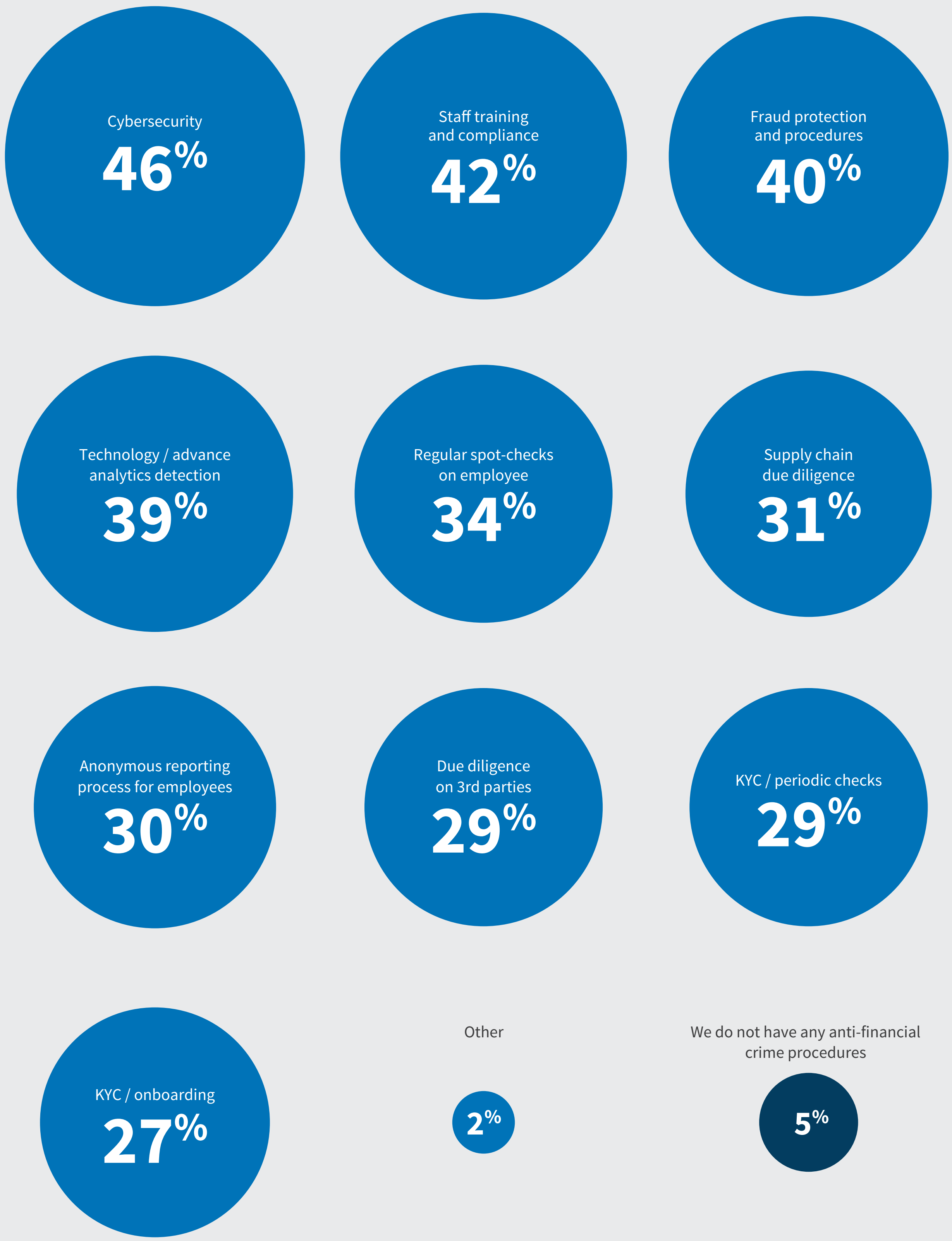
In the face of emerging threats, companies expect to increase their compliance spend by 22% in 2020, with nearly half of respondents saying cybersecurity is their highest priority. They will increase investment in cybersecurity, advanced analytics, screening for employee onboarding, supply chain due diligence, third-party due diligence and Know Your Customer (KYC) compliance procedures.

“By embracing purpose-driven, ethically-based systems such as anti-money laundering, companies are not only less vulnerable to penalties and sanctions, they build reputational resilience amongst consumers who really care about these issues.”

ALMIRA CEMMELL
Senior Managing Director, Forensic & Litigation Consulting

PREVENTING FINANCIAL CRIMES

Q. Which of the following has or are you expecting to happen to your company in your country?



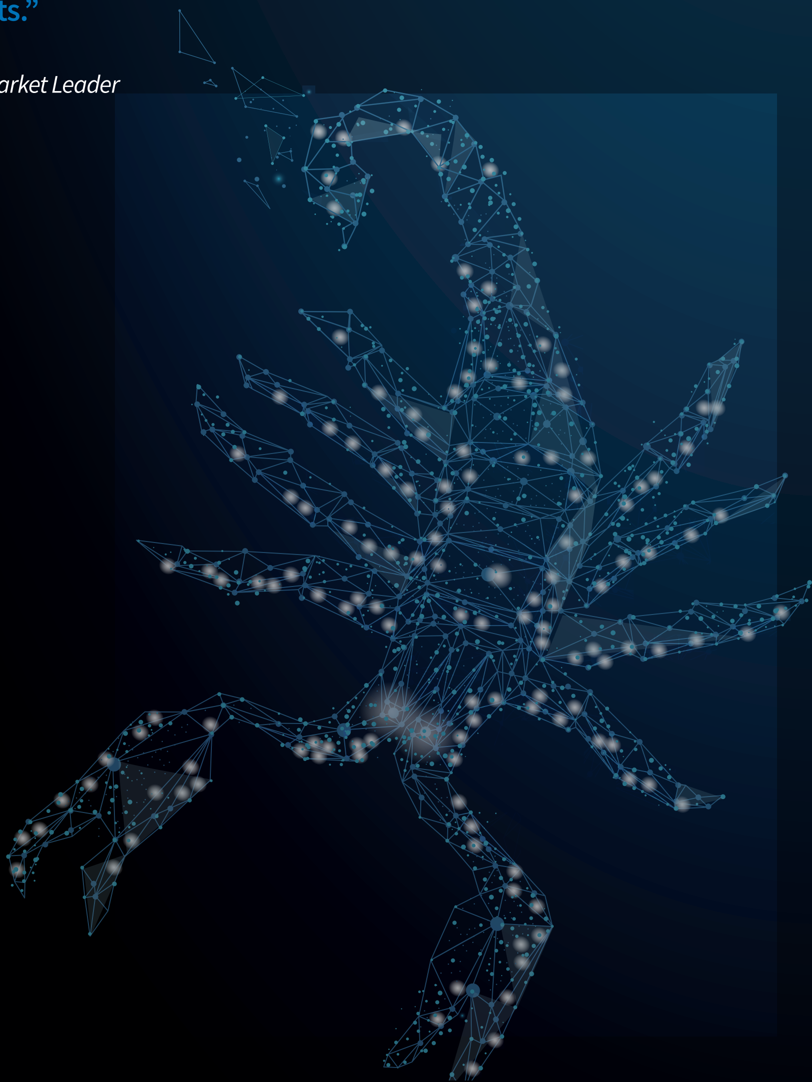
64%

OF RESPONDENTS HAVE BEEN EXPOSED TO FINANCIAL CRIME IN 2019

"Not only are new technologies such as artificial intelligence, machine learning and blockchain enabling companies to enhance resilience by more accurately predicting company risks and proactively addressing financial fraud in a world of exponentially expanding data, they are also being used by perpetrators of financial crimes to penetrate companies and misappropriate their digital and other corporate assets."

EDWARD WESTERMAN

Senior Managing Director, Global Investigations Market Leader



ftiresiliencebarometer.com

#ResilienceBarometer

Sustainability: Engaging for growth

Companies are increasingly expected to play a lead role in addressing environmental, social and governance (ESG) issues that have traditionally been the preserve of governments. The most resilient companies have embedded sustainability into their business models and decision-making structures and engage with a range of stakeholders to prepare for related risks.

As the investment community continues to integrate sustainability issues into their investment criteria, ESG ratings and performance will increasingly be top-of-mind for executives.

Whether this is as a direct result of a positive ESG score, pro-active future proofing of the company or perception of the leaders, the impact on value is considerable.

Our findings show that companies tend to be more positive about their efforts to address social issues rather than environmental issues by an average margin of 8%. Of those companies that reported their materiality/sustainability activities, most focused on social issues, rather than environmental factors: consumption (65%); employee health and safety (60%); labour practices (54%); anti-corruption practices (53%) and management of the legal and regulatory environment (52%).

The Financial Services industry, as a key focus for regulators, has been feeling the most pressure on ESG issues over the past year, particularly in Europe. As a result of industry convergence, the Financial Services sector plays a key part in extended value chains and G20 leaders expect a ripple effect to drive change across other markets. Supply chains will continue to be disrupted as pressure mounts for companies to become more transparent and proactive in managing ESG risks.

TOP FIVE ESG TOPICS DISCLOSED IN 2019	
1	Energy consumption
2	Employee health and safety
3	Labour practices
4	Anti-corruption practices
5	Management of the legal and regulatory environment

Almost 40% of respondents in our survey say the biggest pressure to be more transparent about their sustainability strategy comes from regulators, compared to 37% for customers/clients and the more traditional sources of pressure, such as media (19%) and activists or NGOs (13%).

Despite the consumption of materials and resultant waste now clearly linked to the climate agenda, only one in four companies reported on circular business models – a solution for improving resource management and decreasing waste production. Yet 78% of respondents rate their companies favourably in this regard, suggesting some companies are missing an opportunity to positively position their businesses through reporting on this issue.

Of the main ESG issues, employee diversity continues to rank highly, with 89% of executives surveyed believing this is favourable and 74% rating it as important for their business.

Likely upcoming trends in ESG compliance include mandatory reporting of gender pay gap information; diversity and ethnicity inclusion targets and performance; as well as recycling and environmental targets.

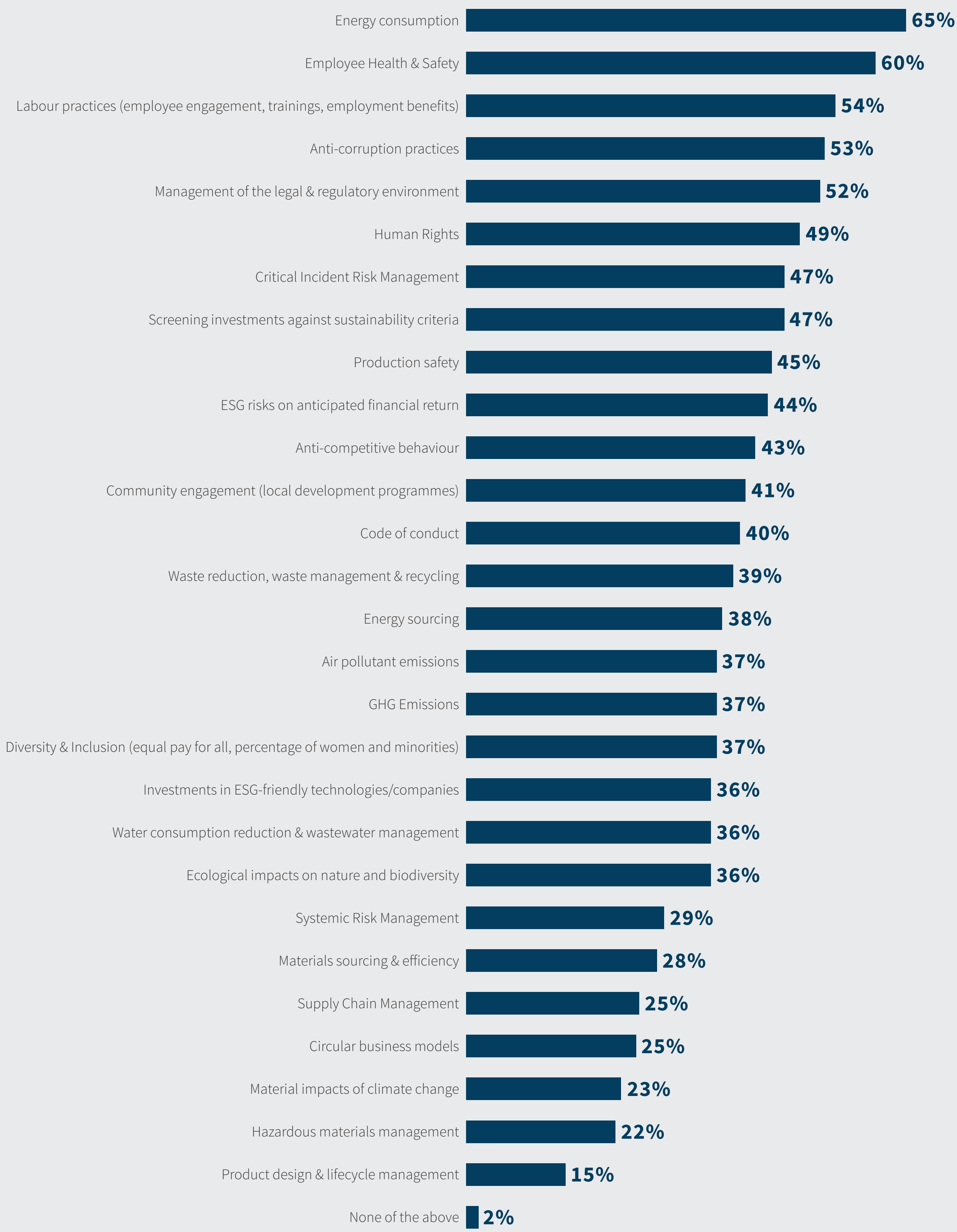
Businesses demonstrating their resilience in these areas will be those that get ahead of the curve by improving their ESG reporting, driving greater disclosure and preparing for increased transparency on sustainability factors.

STAKEHOLDERS REQUESTING TRANSPARENCY

Q. Which of the following stakeholders have been requesting more transparency about your company's sustainability strategy in the last 12 months?

DISCLOSURE TOPICS REPORTED

Q. Which of the following materiality disclosure topics does your company report upon?



39%

OF RESPONDENTS SAY THE BIGGEST PRESSURE TO BE MORE TRANSPARENT COMES FROM REGULATORS

"It's no longer possible for companies to trade off their good performance on one sustainability measure with their underperformance in another. Just because a company performs well on addressing social concerns, doesn't mean it shouldn't prepare for environmental risks. Sustainability issues need to be embedded in a company's business strategy in a comprehensive and holistic way."

MARTIN PORTER
Senior Advisor, Strategic Communications

Cybersecurity: Resilience requires proactivity

The complex and ever-changing nature of cyber risk requires a continued evolution in how organisations approach resilience. No longer is access constrained to the four walls of an organisation. Any connected entity can serve as a point of entry, including third-party vendors who act as a "back door" to larger enterprise networks. Responding effectively to cyber risk requires proactive and holistic management helping mitigate threats, reduce downtime, and protect an organisation's reputation.

"A cyber breach is a matter of "when" and not "if." You can't control the timing, but you can get ahead of the threat by preparing your defence. Developing a plan involving your people, processes and technologies for when that moment arrives is key to achieving cyber resilience."

JOSHUA BURCH
Senior Managing Director
Head of Cybersecurity, EMEA

The cyber risk landscape is dynamic and fluid, leaving organisations with stagnant policies and procedures vulnerable to attack. Just as threats increase in sophistication and malicious actors learn to bypass protections, organisations must continually assess and modify their cyber resilience methodology to keep pace. Our research shows that at least one in four G20 organisations have experienced a cyber attack, where assets were stolen or compromised, in the last 12 months, emphasising the need for improved security.

Further examining those negatively impacted by cyber attacks, lost revenue, reputation damage, and lost customers were the top three impacted areas. A single cyber incident can tarnish how an organisation is publicly viewed, especially if the situation is not managed carefully. However, proactive reputation management and transparency with the public can leave an organisation in a better light post-incident, instead of succumbing to the potentially long-lasting negative effects that often are associated with a breach.

Our research shows that social engineering – including phishing – is the most common attack vector, with 27% of large companies researched reporting being negatively impacted as a result in the past 12 months. These incidents do not occur in isolation. Over a third of organisations who have been impacted by a loss of customer/patient data have also lost third party information and have been victims of phishing/social engineering.

The cascading effects of a cyber attack increase the potential damages and fallout organisations face from being unprepared. Resilience requires a complete cyber risk mitigation strategy, which includes understanding each organisation's unique cyber risk profile, maintaining organisation-wide cybersecurity awareness, identifying critical assets and developing and testing a business continuity and incident response plan. There is room for improvement in this area however. Less than half of G20 organisations we surveyed reported to manage cyber attacks proactively, and only 10% believe they have no cybersecurity gaps at all.

Shifting to a proactive mindset when attempting to mitigate cyber risk and become resilient can begin with an organisation's first line of defence – their people. Our research shows that 28% of G20 organisations believe 'employee awareness, security, culture and training' are their biggest security gaps, and 35% have invested in this area over the past 12 months. People can be the weakest link in the security chain, or organisations can invest in their own staff and turn them into their strongest asset.

Beyond creating a "culture of security," organisations must proactively assess their digital ecosystem to determine additional vulnerabilities. Malicious actors often look for weak spots as access points and they can leverage connected third parties to gain entry to their primary target. Despite vendors serving as an entry point for hackers, only 35% of those surveyed reported to screen suppliers/clients/other parties, versus 42% in 2019. Cyber resilience involves the protection of internal assets, in addition to identifying and closing any gaps that connected external parties present.

20%

OF COMPANIES WERE VICTIMS OF A RANSOM OR DATA HOSTAGE SITUATION IN 2019

Building a resilient organisation also requires proactive coordination from multiple departments, including senior leadership, instead of leaving cybersecurity to the IT department to handle independently. This holistic approach allows for cybersecurity to be considered as part of strategic decisions, instilling it from the outset versus attempting to address it later. Our research shows that at least half of G20 organisations heavily involve their Board of Directors, Operations, C-Suite, Strategy, or General Counsel/ Legal/Compliance departments in proactive cybersecurity planning. While there is increased recognition by senior leaders that cybersecurity is a business-critical risk, there is room for improvement in this area and resilience is unachievable without their input and buy-in.

NEGATIVE IMPACT

Q. What was the negative impact as a direct consequence of these cyber attacks?

27%	25%	24%	20%	20%	18%	17%	16%	16%
Lost revenue	Reputation damage	Lost customers	Loss of value (stock market value)	Management attention was diverted	Employees left	Fine from regulator	Litigated against	New hires decided not to join

2% Other | **27%** There was no negative impact

SECURITY GAPS VS INVESTMENTS

Q1. Which of the following have you invested in over the past 12 months?
Q2. Where do you believe your biggest cybersecurity gaps are? (Please select all that apply)

Technology: Transforming business models to ensure future business resilience

Digital disruption is an all-pervasive trend that presents companies with an opportunity to transform their business models to drive long term success. Resilient companies optimise their planning decisions by making technology transformation a strategic priority.

Our research shows that over the next 12 months, 80% of senior executives rated their company as being under extreme or significant pressure to integrate technology and innovation into their business. The impetus for corporates to respond to the changing digital environment by transforming their business and demonstrating their technological relevance has never been greater.

Moreover, with 68% of respondents concerned that they will only have five years to remain competitive if they do not make the necessary investments in technological transformation, there is increasing recognition from senior business leaders that integrating technological transformation into a company's business model is an imperative. This goes beyond just creating a competitive advantage, it is a matter of corporate survival.

Across industries, transformative technologies such as artificial intelligence, blockchain, 5G and Internet of Things are disrupting the way companies, big and small, international and domestic deliver new and existing products and services. Not only is it about competing more effectively, managing costs, protecting and using customer data, but ultimately it is about how companies can retain the trust of customers. Importantly, it is also changing the way companies manage their workforces and continues to impact their culture and leadership.

"The real opportunity for companies embracing the Fourth Industrial Revolution is to look outwards, beyond the transformation of their own business. To be resilient in the future, companies need to unlock the true potential of innovation by collaborating across digital ecosystems."

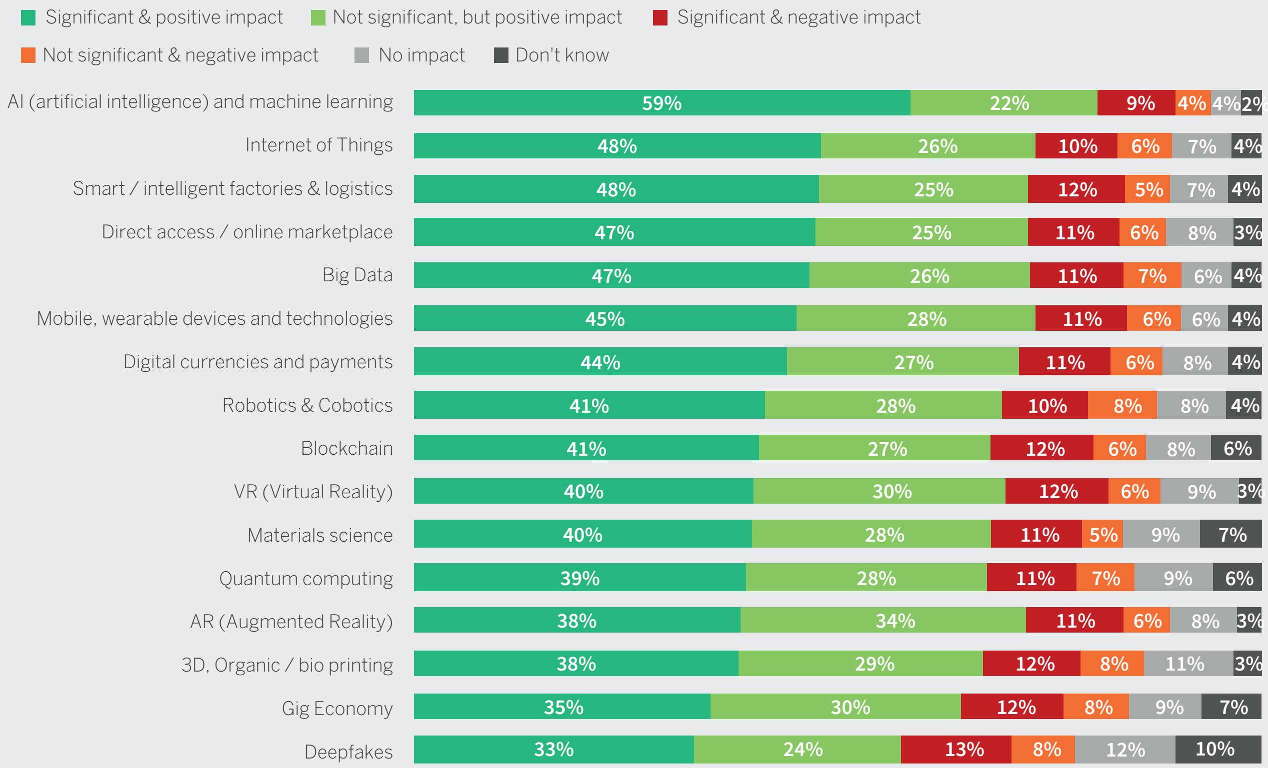
CHARLES PALMER
Senior Managing Director, Global Head of TMT, Strategic Communications

Our survey shows that sectors such as Resource Transformation (Industrials & Chemicals) and Healthcare need to be the most innovative to keep pace with rapid technological changes, although executives across all industries report this as an emerging threat for their businesses.

The potential benefits of innovation investment are often clear, but the challenges come in multiple forms.

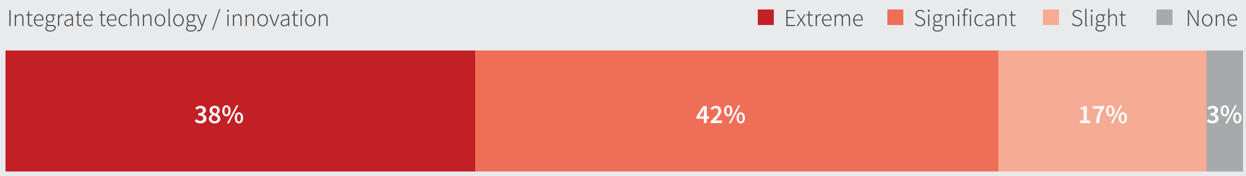
PERSONAL ATTITUDES TOWARDS TECHNOLOGY

Q. Which of the following do you consider will have the greatest impact on your industry within the next 10 years?



COMPANY PRESSURES OVER NEXT 12 MONTHS

Q. How would you generally rate the pressure upon your company to achieve the following over the next 12 months?



New business models present new risks, particularly around cybersecurity, data privacy and regulatory changes, as well as the more predictable operational and supply chain risk. Resilient companies are those that adapt their security and risk management practices to enable them to successfully prepare in a hyper-connected business environment.

59%

OF RESPONDENTS BELIEVE AI & MACHINE LEARNING WILL IMPACT SIGNIFICANTLY OVER THE NEXT 10 YEARS

While C-suite executives may not personally have the technical knowledge around advanced technologies, our findings show that they are not averse to using new technologies in transforming their businesses. Of those leaders surveyed, 59% say artificial intelligence and machine learning will have the most significant impact on their industry over the next 10 years. Of these, 81% believe this to be positive, in line with last year's 82%.

Research Methodology

The 2020 FTI Consulting Resilience Barometer incorporates the views of 2,276 respondents from large companies across all G20 countries.

The quantitative survey was conducted in November 2019 and respondent profiles replicate those used in last year's research. The majority (74%) of respondents were C-suite and senior managers executives from privately owned companies (2019: 77%), while 26% were from publicly listed entities (2019: 23%).

There was a strong correlation between the global turnover reported between 2019 and 2020 surveys, with respondents reporting an average global turnover of USD 17,439 million (2019: 19,162 million) over the past 12 months. Companies reporting a global turnover of USD 1 billion over the past 12 months comprised 10% of the sample size (2019: 8%), while those reporting more than USD 100 billion made up 7% (2019: 4%) and those reporting USD 100 million made up 7% (2019: 6%). In total, participating companies employ a global sum of 58 million people, employing an average of 23,336 people (2019: 22,357).

Membership of the G20 consists of 19 individual countries plus the European Union. The EU is represented by the European Commission and by the European Central Bank. Collectively, the G20 economies account for around 90% of the Gross World Product; 80% of world trade and two-thirds of the world population[1].

Each country's results have been weighted so that each country represents a similar proportion in the total 'G20' results. The results were also weighted so that the industry breakdown of each country is similar to the breakdown of the 2019 survey.

Please note that the standard convention for rounding has been applied and consequently some totals do not add up to 100%.

Further information on the results and methodology can be obtained by contacting
Dan.Healy@fticonsulting.com

"Complacency by leadership is the real threat to companies. By not proactively preparing for these 18 foreseeable scenarios, leaders will be arguably complicit in increasing the already significant time they spend on crisis situations as opposed to building their preparedness for the future."

DAN HEALY
Managing Director, Head of Research, Strategic Communications

KEY BUSINESS SCENARIOS INCORPORATED INTO THE RESILIENCE SCORE

01. Regulatory and geopolitical disruption
- Regulatory fine
- Trade restrictions
- Embroiled in a regulatory (or other) investigation
- Impacted by sanctions
- Political disruption or abrupt policy changes

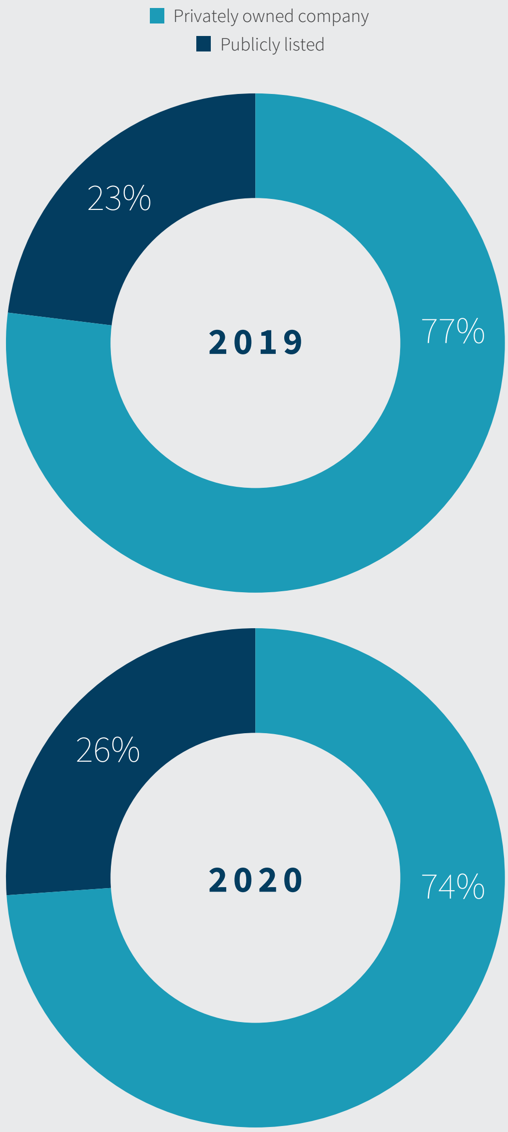
02. Adapting to change & business model resilience
- Major product defect
- Cash flow issues from bad debt
- An operational failure that causes major environmental damage
- Major new competitor entering the market
- Impacted by disruptive technology

03. Leadership, culture and communication
- Victim of fraudulent practices
- Embroiled in political corruption
- Leadership change / transition
- Leak of sensitive internal communications

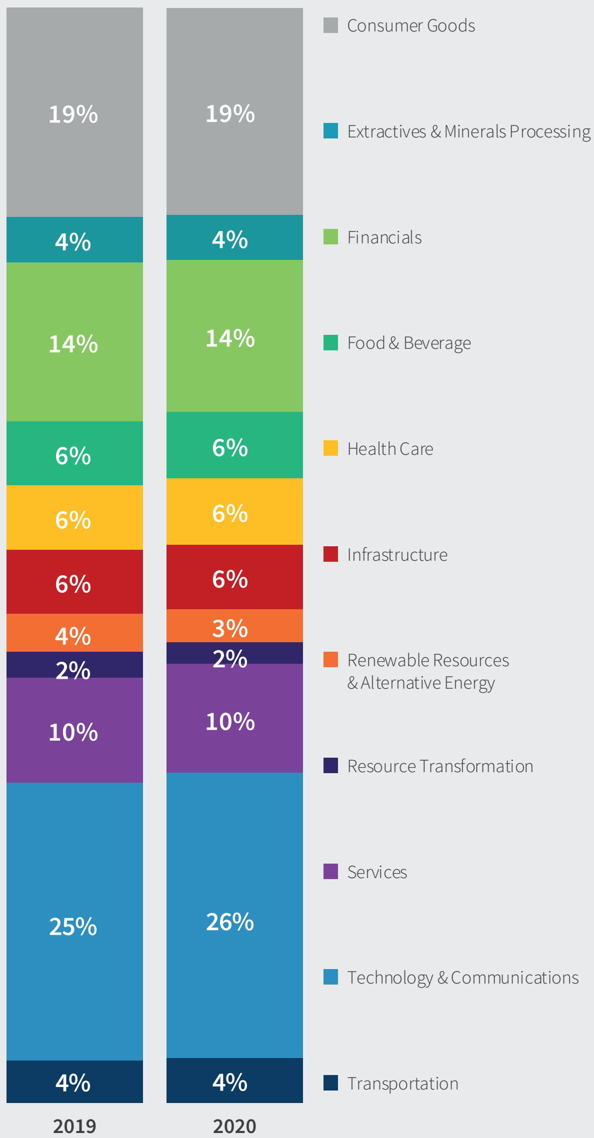
04. Protecting against new threats in a digital world
- Litigated against
- Cyber attacks stealing or compromising assets
- A target of aggressive M&A activities
- Disrupted by stakeholder activism

1 https://www.g20foundation.org/g20/what-is-the-g20

ORGANISATION TYPE



INDUSTRY CLASSIFICATION



About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes.

Operating globally across 27 countries on six continents, we offer a comprehensive suite of services designed to assist clients right across the business cycle – from proactive risk management to the ability to respond rapidly to unexpected events and dynamic environments.

www.fticonsulting.com

CORPORATE FINANCE AND RESTRUCTURING

- Business Transformation
- Turnaround & Restructuring
- Transactions
- Valuation & Financial Advisory
- Dispute Advisory
- Tax
- Executive Compensation & Corporate Governance

ECONOMIC AND FINANCIAL CONSULTING

- Antitrust and Competition Valuation
- Intellectual Property
- International Arbitration
- Labour and Employment
- Public Policy
- Regulated Industries
- Securities Litigation & Risk Management
- Centre for Healthcare Economics and Policy
- Economic Impact & Market Modelling

FORENSIC AND LITIGATION CONSULTING

- Forensic Accounting and Advisory Services
- Global Risk & Investigations Practice
- Dispute Advisory Services
- Trial Services
- Compliance, Monitoring and Receivership
- Anti-Corruption Investigations & Compliance
- Anti-Money Laundering
- Export Controls & Sanctions

STRATEGIC COMMUNICATIONS

- M&A, Crisis Communications & Special Situations
- Capital Markets Communications
- Corporate Reputation
- Public Affairs & Government Relations
- People & Change
- Digital & Insights
- Strategy Consulting & Research

TECHNOLOGY

- E-Discovery Consulting
- Managed Document Review
- Collections & Computer Forensics
- Information Governance, Privacy & Security
- Contract Intelligence
- Radiance Visual Analytics Software
- Strategic IT

SPECIALIST SERVICES

- Cybersecurity
- Private Capital Advisory
- Office of the CFO
- Activism and M&A Solutions
- Family Enterprise Services
- Applied Statistical Data Sciences& Data & Analytics

Our Experts

JOSHUA BURCH
Senior Managing Director
Head of Cybersecurity, EMEA
Forensic & Litigation Consulting
Joshua.Burch@fticonsulting.com

ALMIRA CEMMELL
Senior Managing Director
Forensic & Litigation Consulting
Almira.Cemmell@fticonsulting.com

CAROLINE DAS-MONFRAIS
Senior Managing Director
Chief Strategy Officer, EMEA
Caroline.Das-Monfrais@fticonsulting.com

ALEX DEANE
Senior Managing Director
Head of Public Affairs UK
Strategic Communications
Alex.Deane@fticonsulting.com

NEIL DOYLE
Senior Managing Director
Strategic Communications
Neil.Doyle@fticonsulting.com

JOHN ELLISON
Senior Managing Director
Economic & Financial Consulting
John.Ellison@fticonsulting.com

JULIA HARRISON
Senior Managing Director
Global Head of Public Affairs & Government Relations, Strategic Communications
Julia.Harrison@fticonsulting.com

DAN HEALY
Managing Director, Head of Research
Strategic Communications
Dan.Healy@fticonsulting.com

JAMES MELVILLE-ROSS
Senior Managing Director
Strategic Communications
James.Melville-Ross@fticonsulting.com

STELLA MENDES
Senior Managing Director
Co-Leader of Financial Services
Forensic & Litigation Consulting
Stella.Mendes@fticonsulting.com

SIMON LEWIS
Vice Chairman in EMEA
Global Head of Financial Services
Strategic Communications
Simon.Lewis@fticonsulting.com

CHARLES PALMER
Senior Managing Director
Global Head of TMT
Strategic Communications
Charles.Palmer@fticonsulting.com

ANDREW PIMLOTT
Senior Managing Director
Forensic & Litigation Consulting
Andrew.Pimlott@fticonsulting.com

MARTIN PORTER
Senior Advisor
Strategic Communications
Martin.Porter@fticonsulting.com

EDWARD WESTERMAN
Senior Managing Director
Global Investigations Market Leader
Edward.Westerman@fticonsulting.com

Notes

ftiresiliencebarometer.com
#ResilienceBarometer

EXPERTS WITH IMPACT