DATA-FIRST THINKING

GLOBAL RISK AND COMPLIANCE REPORT 2021

How data, technology and collaboration are reshaping risk

REFINITIV®

An LSEG Business

REFINITIV®

WORLD-CHECK®

For best-in-class risk intelligence think Refinitiv World-Check.

Helping you simplify your customer and third-party risk screening and meet your regulatory obligations.

Our quality data, technology and human expertise has been trusted by our customers for over two decades to help them make informed decisions.

Find out how we can help you.

Refinitiv.com

REFINITIV®

An LSEG Business

FOREWORD

Phil Cotter
Group Head, Customer & Third Party Risk Solutions, Data & Analytics, Refinitiv

Our survey reveals how the Covid-19 pandemic has significantly raised customer and third-party risks, but also highlights the potential of technology to reshape them.

With a global death toll that has surpassed three million in 2021, the Covid-19 pandemic has changed the world forever. For businesses and their employees, it continues to create severe day-to-day pressures, from keeping vital operations running to rebuilding fractured supply chains. In this environment, it is perhaps not surprising that organisations have found it harder to focus on third-party risks, resulting in more opportunities for criminals to defraud consumers and companies.

Taking shortcuts

Our survey reflects companies' difficulties, with 65% of respondents agreeing that the pandemic has forced them to take shortcuts with know your customer (KYC) and due diligence checks. Although Covid-19 has been extremely disruptive, compliance gaps had been a persistent problem long before the pandemic. Our 2019 risk survey found that 49% of third-party relationships had been subject to due diligence checks, compared to 44% in 2021. On a more positive note, our current survey shows a growing awareness of environmental, social and governance (ESG) factors and green crime, suggesting that the pandemic may have created a turning point.

Technology and data show us the way

By heightening and exposing risks, the pandemic is also helping organisations to address them. The best way to do so is clearly highlighted by our survey: technology, data and automation are not only enablers, they can also act as transformers. Organisations which use innovative technologies are not just better protected from customer and third-party risk, they are more aware of them and crucially are more likely to continue investing in further prevention and mitigation.

Collaboration is key

Another key trend seen during the pandemic has been greater collaboration – whether it's between businesses, people or institutions – for the common good. Here, we find that those already using technology to combat financial crime are 60% more likely to collaborate with enforcement agencies than those not using such technology. This gives us renewed hope that the collaborative approach which we have long championed at Refinitiv – between enforcement agencies, innovators and non-governmental organisations, to name but a few – can be strengthened by recent events and enable us to forge a safer future, together.

Join the conversation #FightFinancialCrime and #FightGreenCrime

ABOUT THE REPORT

This report is based on research commissioned by Refinitiv that was conducted online by an independent consulting company during March 2021. A total of 2,920 managers in large organisations, who are either knowledgeable or involved in regulatory compliance and practices, completed the survey.

This research was conducted across 30 countries, but the survey respondents' headquarters and third-party relationships are truly global. Weighting was applied to each country to ensure equal representation. Please note that the standard convention for rounding has been applied, and consequently some totals do not add up to 100%.

We also make reference in the report to an earlier Refinitiv innovation in financial crime survey conducted in March 2019 across 24 countries and a Refinitiv third-party risk survey conducted in February 2020 across 16 countries. When using this earlier surveys for comparison, we do so on a like-for-like country basis.

COUNTRY BREAKDOWN OF RESPONDENTS

	TOTAL	USA	Canada	Brasil	Argentina	Mexico	United Kingdom	Germany	France	Netherlands	Italy	Spain	Russia	Poland
2021	2920	106	107	110	110	110	108	107	110	103	109	109	110	109
2019	3138	130	129	130	130	130	130	128	130	105	130	130	130	122

NET Nordics	Australia	China	Hong Kong	India	Singapore	South Korea	Japan	Turkey	UAE	Saudi Arabia	South Africa	Nigeria
207	107	109	107	110	110	108	104	110	110	110	110	110
220	129	130	118	130	130	n/a	n/a	130	127	129	122	119

BREAKDOWN BY JOB ROLES/SENIORITY

20% C-suite

39% Senior management

41% Middle management

BREAKDOWN BY TURNOVER

Our survey respondents work for organisations with an average of

US$24.3BN / £17.2BN

annual turnover

DEFINITION

WHAT IS FINANCIAL CRIME?

The usual focus of financial crime investigation is on the illicit money flows from crimes such as money laundering, bribery, tax evasion, fraud and corruption that support human abuses including modern slavery, drug trafficking and prostitution.

For the purpose of this report we have taken a wide definition covering all financial crimes to provide as complete a picture as possible on the social and financial impacts.

WHAT IS A THIRD PARTY?

For the purpose of this report we have defined a ‘third party’ as any person or organisation that is connected to a supply chain or is executing business on an organisation’s behalf such as a supplier, distributor, agent and/or partner.

Our definition of the term ‘third-party risk’ includes anything that could expose a company to threats and risks through engagement with third parties including bribery and corruption, modern slavery, environmental crime, wildlife trafficking or conflict minerals.

The term ‘third-party due diligence’ refers to assessment of the third party at the onboarding and ongoing monitoring stage to determine the risk profile.

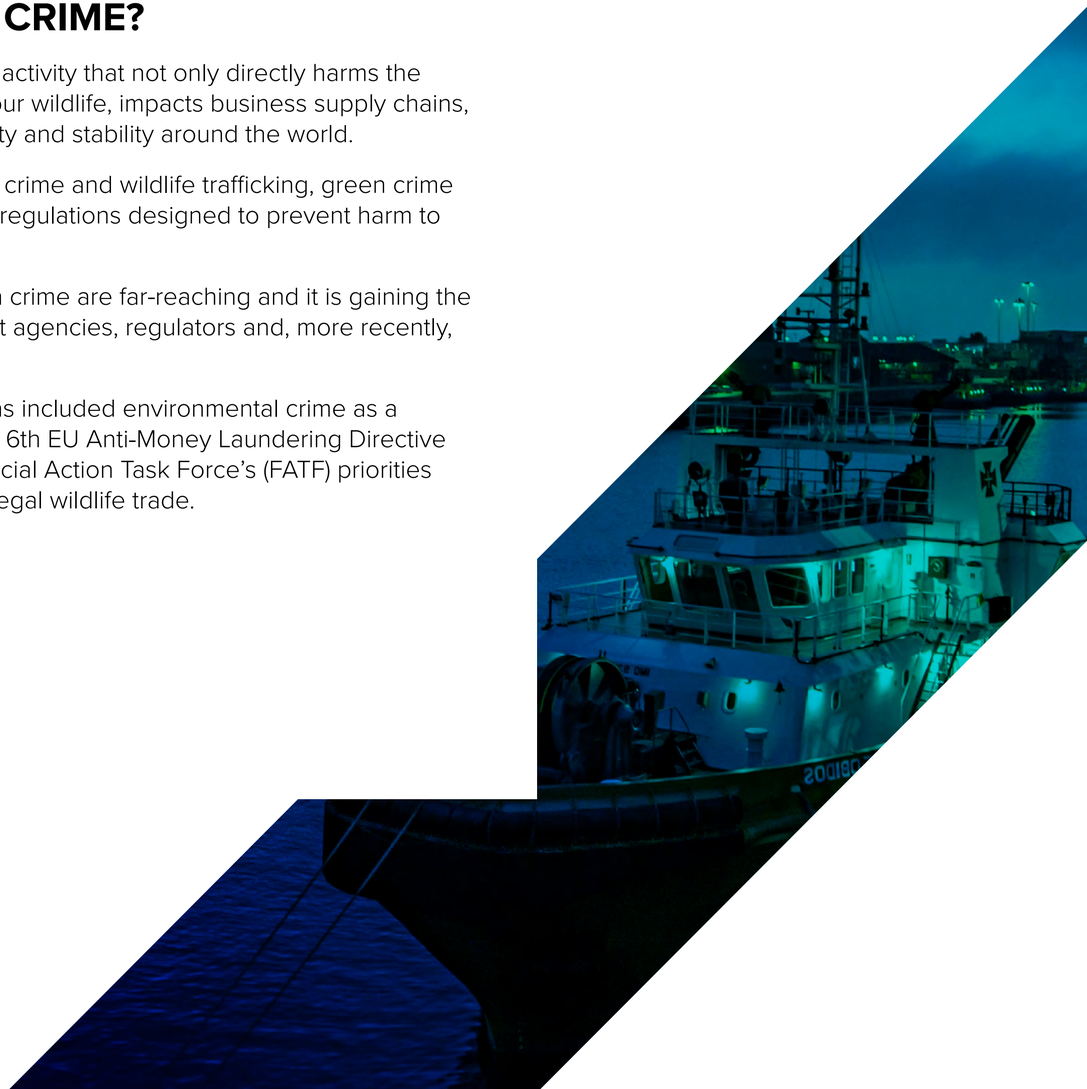
WHAT IS GREEN CRIME?

Green crime involves illegal activity that not only directly harms the environment but threatens our wildlife, impacts business supply chains, and poses a threat to security and stability around the world.

In addition to environmental crime and wildlife trafficking, green crime also includes the flouting of regulations designed to prevent harm to the environment.

The consequences of green crime are far-reaching and it is gaining the attention of law enforcement agencies, regulators and, more recently, the technology sector.

The European Union (EU) has included environmental crime as a predicate offence under the 6th EU Anti-Money Laundering Directive (6AMLD), and the new Financial Action Task Force’s (FATF) priorities for 2020 will focus on the illegal wildlife trade.



HIGHLIGHTS

THE IMPACT OF THE PANDEMIC: AS COMMERCIAL PRESSURES RISE, SO DO RISKS

65% of respondents agreed that the pandemic has forced them to take shortcuts with KYC and due diligence checks

73% of survey respondents were under extreme pressure to increase revenue because of Covid-19

71% of respondents said that cybercrime became more difficult to contain due to Covid-19-related remote working practices

40% of organisations said Covid-19 has made sanctions screening a greater priority

COMPLIANCE GAPS PERSIST: FRAUD, MONEY LAUNDERING AND CORRUPTION

44% of third-party relationships have been through due diligence checks, compared to 49% in 2019

62% of respondents said they were aware of financial crime over the last 12 months, compared to 72% in our 2019 report

64% said they focus more on being regulatory-compliant rather than proactively trying to prevent issues

86% of respondents either use technology to support them with fraud detection or are looking to do so in the future

THE POWER OF INNOVATION: HOW TECHNOLOGIES ARE RESHAPING THE FUTURE OF RISK

86% of respondents agreed that innovative digital technologies have helped identify financial crime

91% of those who use technology in KYC/compliance are looking to improve financial crime detection and mitigation over the next 12 months

60% of those who regularly use technology to prevent risks associated with financial crime are far more likely to have better collaboration with law enforcement agencies than those who don't

45% of respondents believe that application programming interface (API) technology can significantly help reduce the risks associated with financial crime

1 | HOW THE PANDEMIC HAS RESHAPED RISK

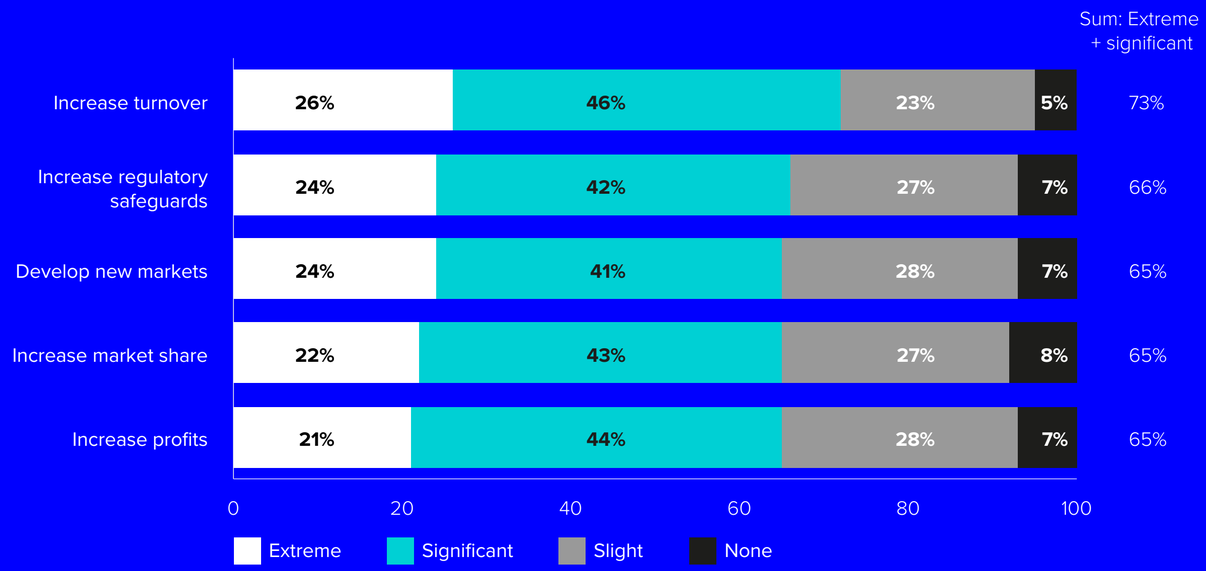
AS THE WORLD CHANGED IN RESPONSE TO THE PANDEMIC, SO DID THE RISK PICTURE

Under-pressure businesses cut corners

The pandemic pushed businesses to the limit. Nearly three-quarters (73%) of survey respondents said they were under pressure to increase revenue and 65% to increase profits because of the Covid-19 pandemic.

Figure 1: PANDEMIC IMPACTS ON COMPANY PRESSURE POINTS

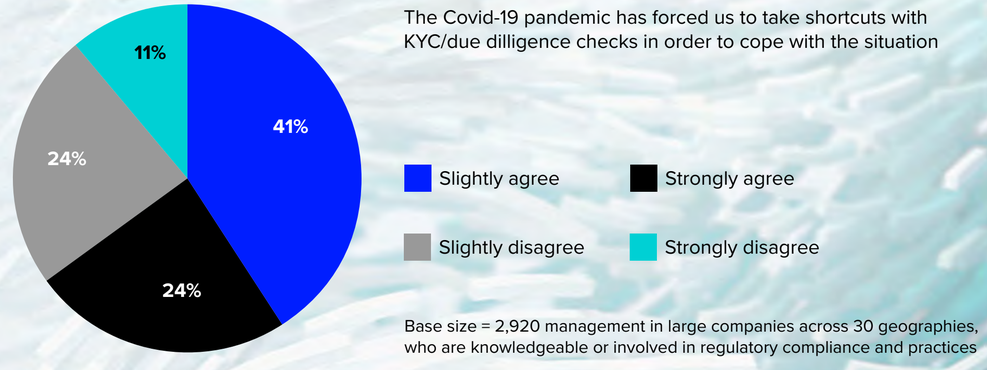
How would you generally rate the pressure upon your company to achieve the following because of the Covid-19 pandemic?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Figure 1b: OPINIONS ON MONITORING EXTERNAL RELATIONSHIPS

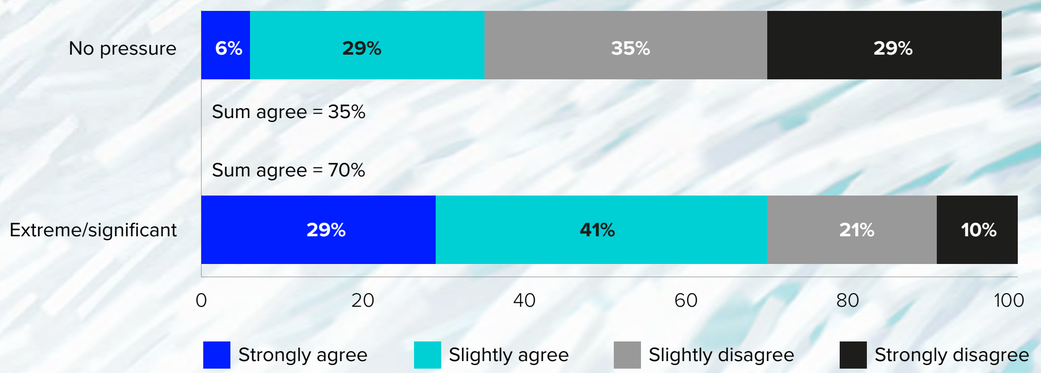
How strongly do you agree or disagree with the following statements?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Figure 2: TAKING SHORTCUTS WITH DUE DILIGENCE

How strongly do you disagree with the following statement? The Covid-19 pandemic has forced us to take shortcuts with KYC/due dilligence checks in order to cope with the situation.



Base size = Those under no pressure: n=139 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

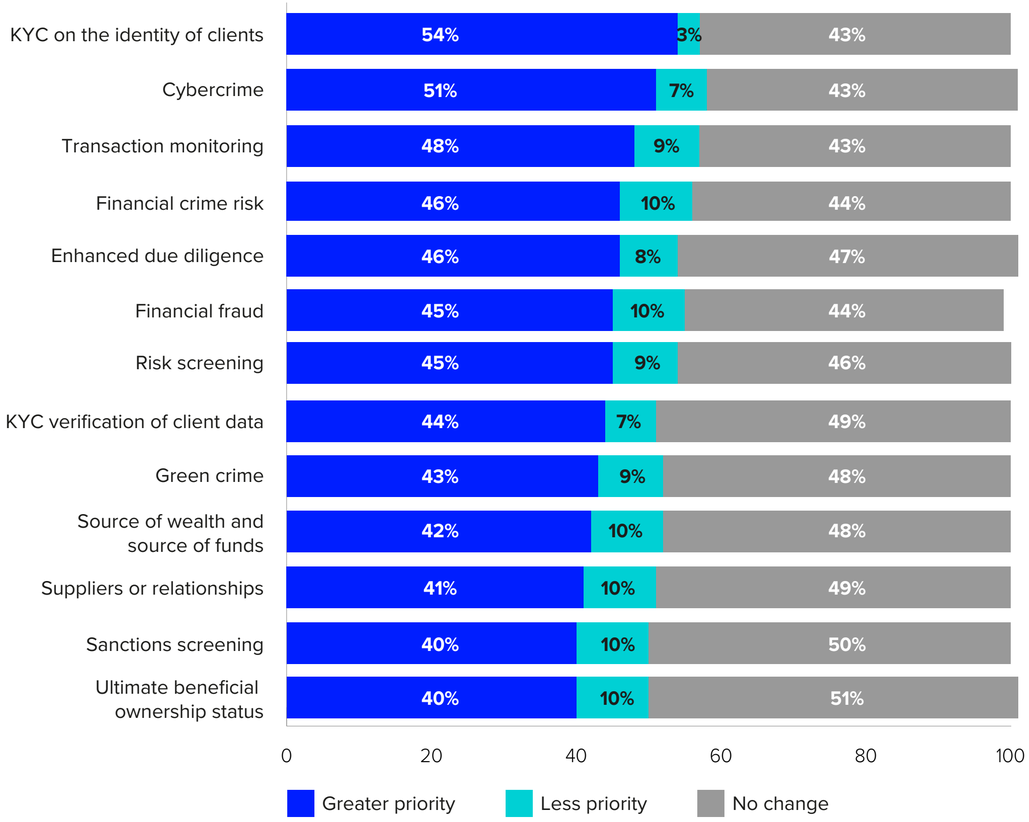
Base size = Those under Extreme/significant pressure: n=2920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practicess

COVID-19 AND KYC COMPLIANCE

Over half (54%) of respondents agreed that Covid-19 had made KYC on the identity of clients a greater priority and 44% said it had impacted the need for KYC verification of client data. The need to repair supply chains and establish new business relationships as a result of Covid-19 may have been a driver behind this renewed focus. Overall, however, 41% (Fig. 3b) of respondents acknowledged that they have not fully managed KYC on the identity of clients, and over half (51%) said that they have not fully run KYC verification of client data.

Figure 3: PANDEMIC IMPACTS ON COMPANY RISK PRIORITIES

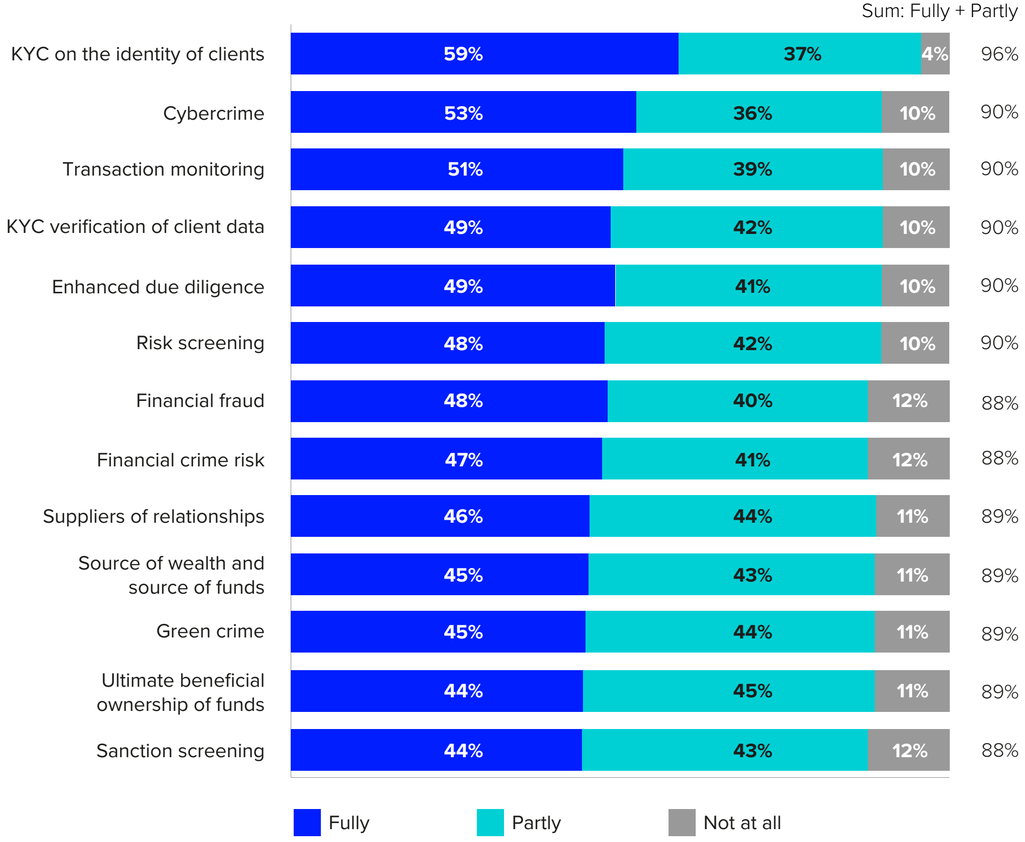
How has the Covid-19 pandemic impacted how your company prioritises the following risks?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Figure 3b: COMPANY RISK MANAGEMENT

How well do you consider your company manages the following risks?



REFINITIV QUAL-ID

POWERED BY WORLD-CHECK

HOW DO YOU KNOW YOUR CUSTOMER IF YOU DON'T KNOW YOUR CUSTOMER?

A powerful combination of digital identity verification, document proofing and risk screening all via API technology

- Faster turnaround times
- Improved accuracy
- Better customer experience
- Streamlined costs

refinitiv.com/qual-id

An LSEG Business

REFINITIV®

SANCTIONS SCREENING

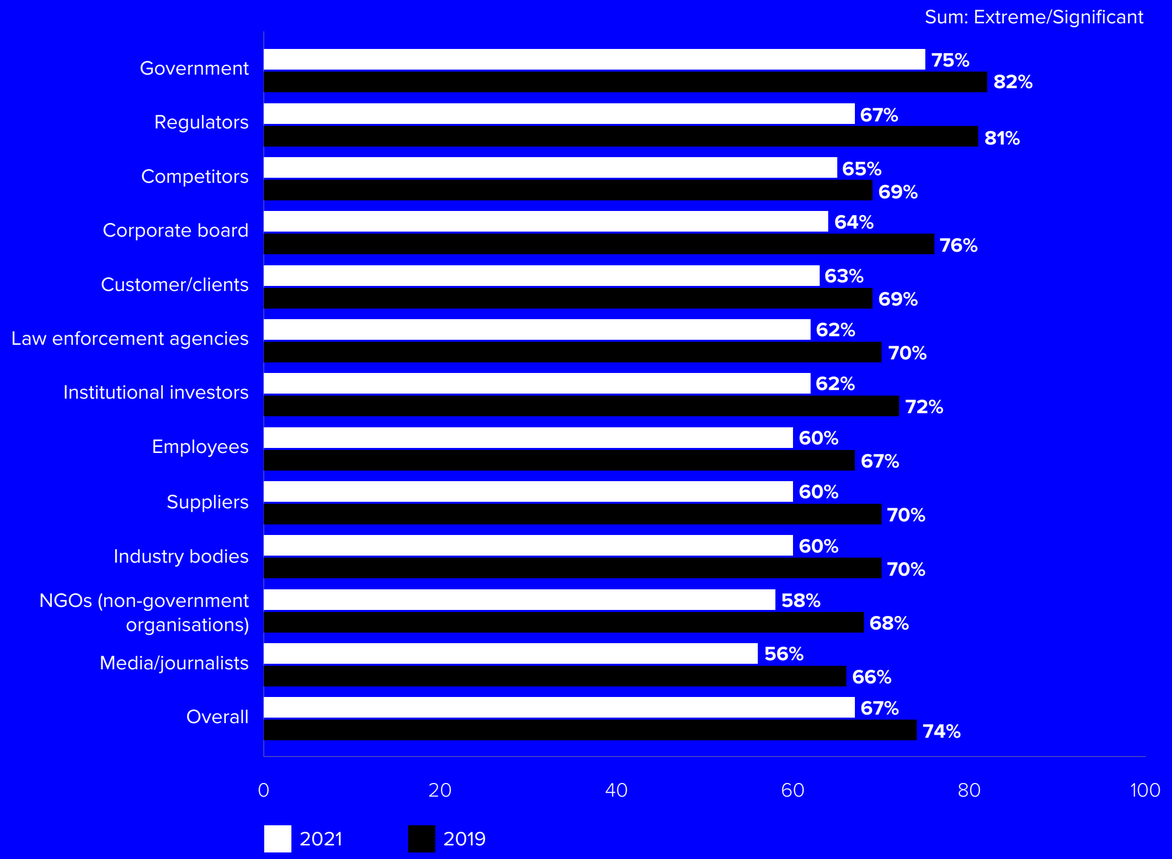
Covid-19 has made sanctions screening a greater priority for 40% of respondents, perhaps again driven by the need to forge new relationships due to the pandemic's impact on supply chains. But this is set against a wider picture of inaction: 56% (Fig. 3b) of respondents said they have not fully managed risks related to sanctions screening. Technology is becoming omnipresent, with 85% of respondents either already using it to support sanctions screening or planning to use it in the future.

GOVERNMENT AND REGULATOR PRESSURES EASE

By directly comparing this year's results with our 2019 risk survey, it is possible to measure changes in the levels of pressure that organisations reported under to prevent financial crime.

Figure 4: PRESSURE TO PREVENT CUSTOMER AND THIRD-PARTY RISK 2019 COMPARISON

How would you generally rate the pressure from the following upon your company to prevent financial crime?



Base size 2021 = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Base size 2019 = 3,138 management in large companies across 24 geographies, who are knowledgeable or involved in regulatory compliance and practices

In our 2021 survey, the pressure coming from governments (75%), regulators (67%) and corporate boards (64%) was significantly lower than in our 2019 survey (82%, 81% and 76%, respectively), suggesting that government focus and resources were directed elsewhere during Covid-19. This is supported by evidence that the Foreign Corrupt Practices Act (FCPA) enforcement actions were at their lowest levels for over 10 years, with only one reported action against a corporate defendant in the first four months of 2021.

FCPA enforcement action: https://fcpablog.com/2021/05/03/why-has-corporate-fcpa-enforcement-stopped/

TECHNOLOGY UPTAKE ACCELERATES

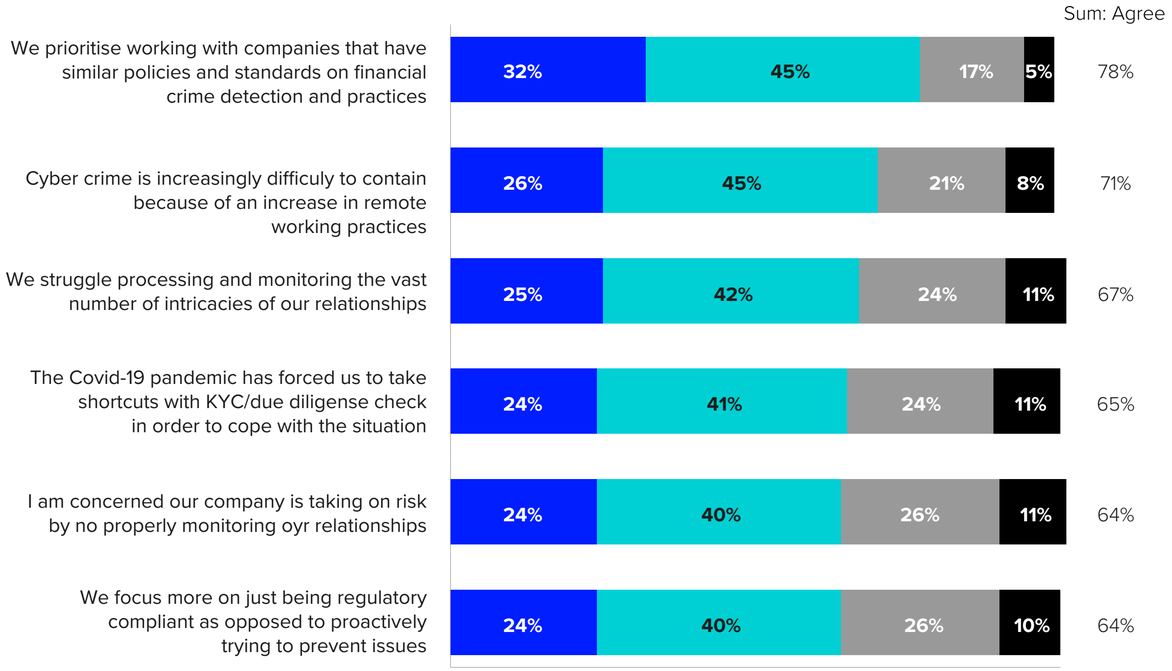
The pandemic appears to be accelerating the investment in technology to fight financial crime. While 43% of those under extreme pressure to increase revenue due to the pandemic said they would like to deploy artificial intelligence (AI) and machine learning to combat financial crime in the future, this fell to just 26% for those that reported they were not under any pressure.

CYBERCRIME RISKS RISE

The ability of global workforces to adapt successfully to remote working was remarkable, but it also opened the door to risks. More than seven in 10 (71%) respondents said that cybercrime has become difficult to contain because of an increase in Covid-19-related remote-working practices. No doubt a reason why 51% (Fig. 3) said that cybercrime had become a greater priority during the pandemic.

Figure 5: OPINIONS ON MONITORING EXTERNAL RELATIONSHIPS

How strongly do you agree or disagree with the following statements?

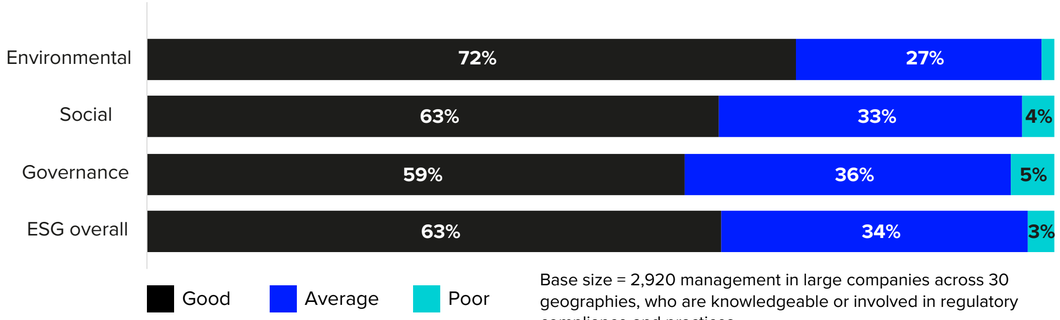


RAISING THE STAKES ON ESG

Covid-19 has proved to be a watershed for the ESG agenda – 43% of respondents said that the pandemic increased the importance of ESG to them overall. This sentiment is likely to continue as regulations, such as the EU Directive on Mandatory Environmental and Human Rights Due Diligence and Germany's upcoming Corporate Due Diligence Act have significant enforcement penalties and require continuous due diligence of third-party relationships.

Figure 6: ESG ELEMENTS

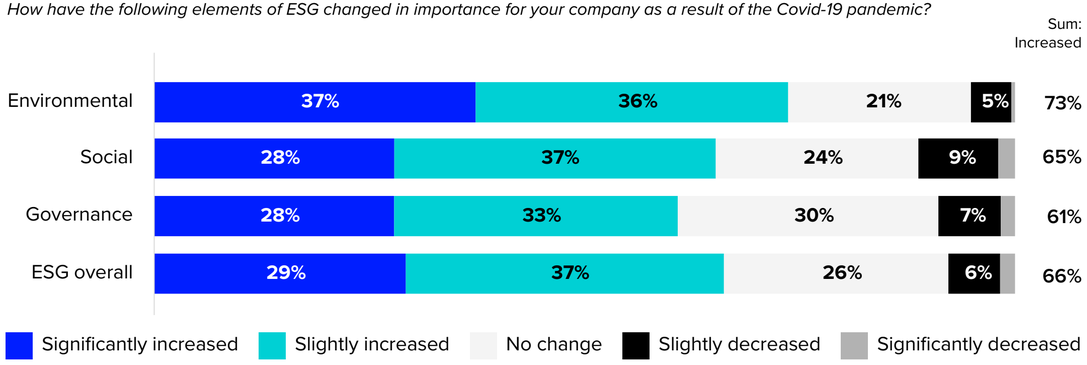
How would you rate your company overall for the following elements of ESG?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Figure 6b: IMPORTANCE OF ESG ELEMENTS

How have the following elements of ESG changed in importance for your company as a result of the Covid-19 pandemic?



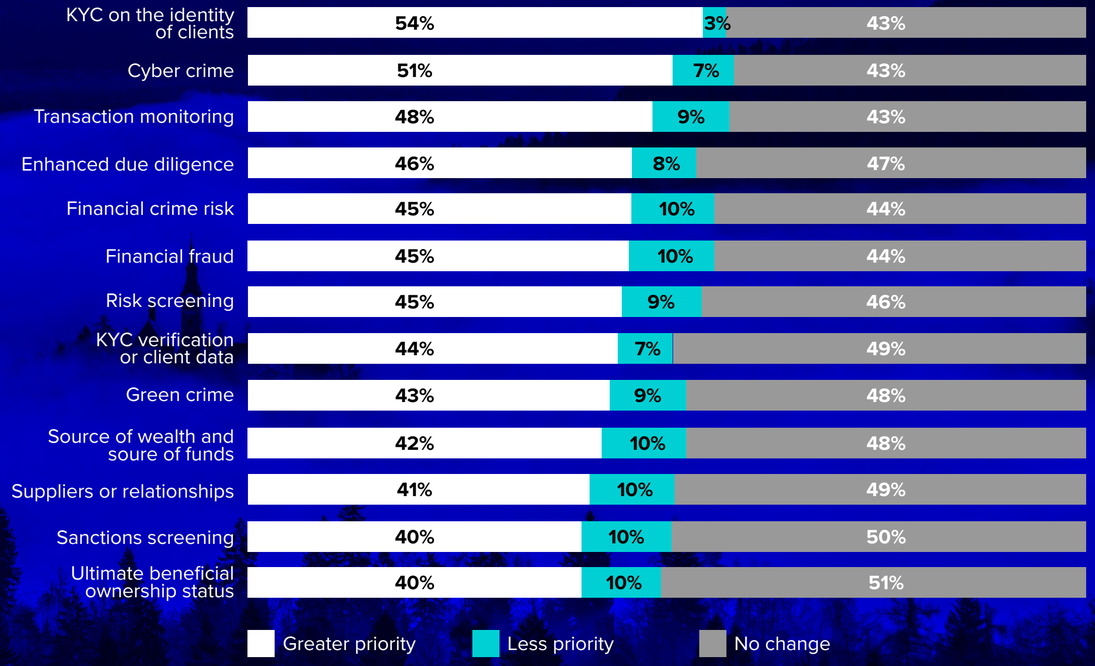
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

GREEN CRIME AWARENESS GROWS

43% of respondents said they now consider green crime, which includes illegal fishing, illegal logging, illegal wildlife trade and waste dumping, as a priority. This is a remarkable finding as a lack of prioritisation and intelligence sharing among law enforcement agencies and policy makers has given the private sector few incentives to focus on it to date. Our 2020 Refinitiv risk survey The Real Risks: Hidden threats within third-party relationships did signal progress however, with 93% of participants stating that if greater enforcement action were taken in relation to third-party risks, they would increase their spending.

Figure 7: PANDEMIC IMPACTS ON COMPANY RISK PRIORITIES

How has the Covid-19 pandemic impacted how your company prioritises the following risks?




PUT ESG THINKING AT THE HEART OF YOUR INVESTMENT PROCESS TO HELP MITIGATE RISK AND MAKE BETTER DECISIONS
Discover more at refinitiv.com/esg
REFINITIV®
An LSEG Business

2 | CLOSING THE COMPLIANCE GAP

OUR SURVEY HIGHLIGHTS PERSISTENT COMPLIANCE FAILINGS BUT REVEALS HOW TECHNOLOGY ADOPTION IS RAISING AWARENESS AND DETECTION

Due diligence drops

Only 44% of respondents said that they conducted initial formal customer or third-party due diligence checks, which is five percentage points below our 2019 findings of 49%. One possible cause for this decline may be a greater difficulty in obtaining the data and legal documentation required to conduct thorough third-party checks. Respondents said that they were only able to obtain 46% of the required information, as opposed to 51% in 2019.

Figure 8.1: DUE DILIGENCE ON EXTERNAL RELATIONSHIPS

What percentage of these relationships did you conduct any initial formal customer or third-party due dilligence check when onboarding them?

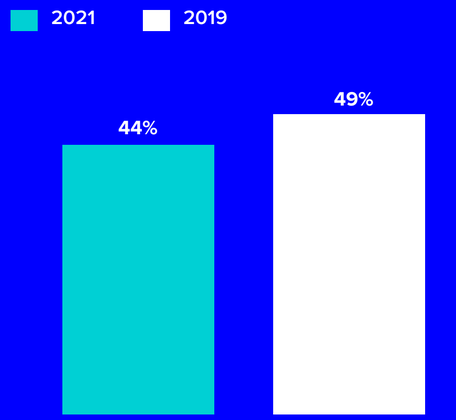
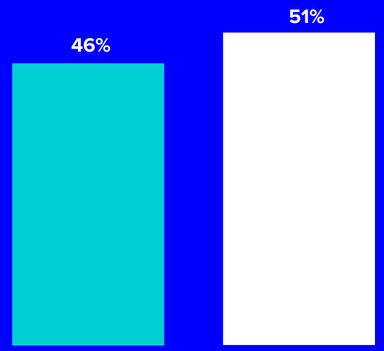
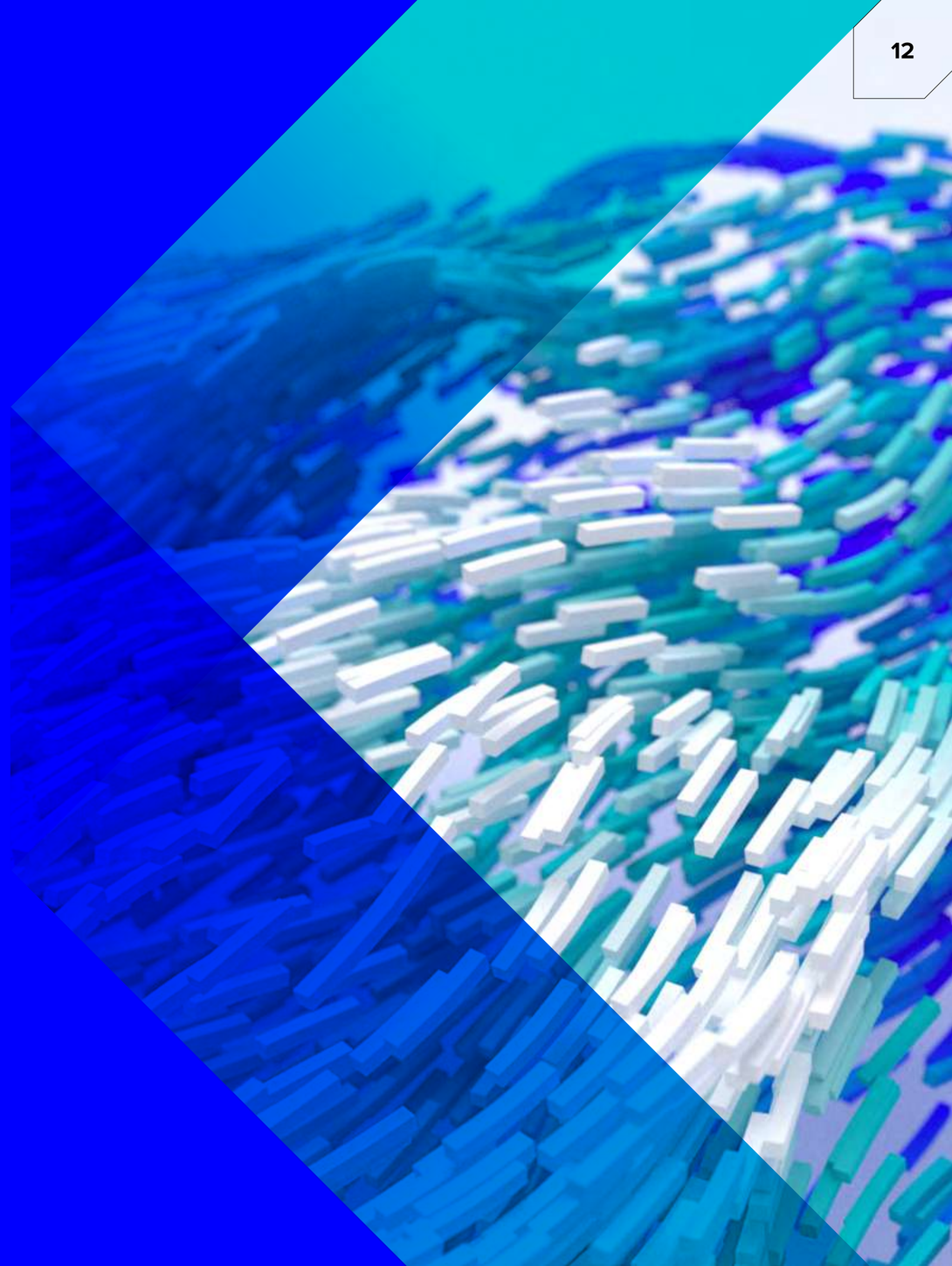


Figure 8.2: ACCESS TO REQUIRED LEGAL DATA

Of the required data and legal documentation in order to conduct a thorough customer or third-party due diligence check with these external relationships, what proportion are you usually able to obtain? (Please select one response)



Base size 2021 = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices
Base size 2019 = 3,138 management in large companies across 24 geographies, who are knowledgeable or involved in regulatory compliance and practices

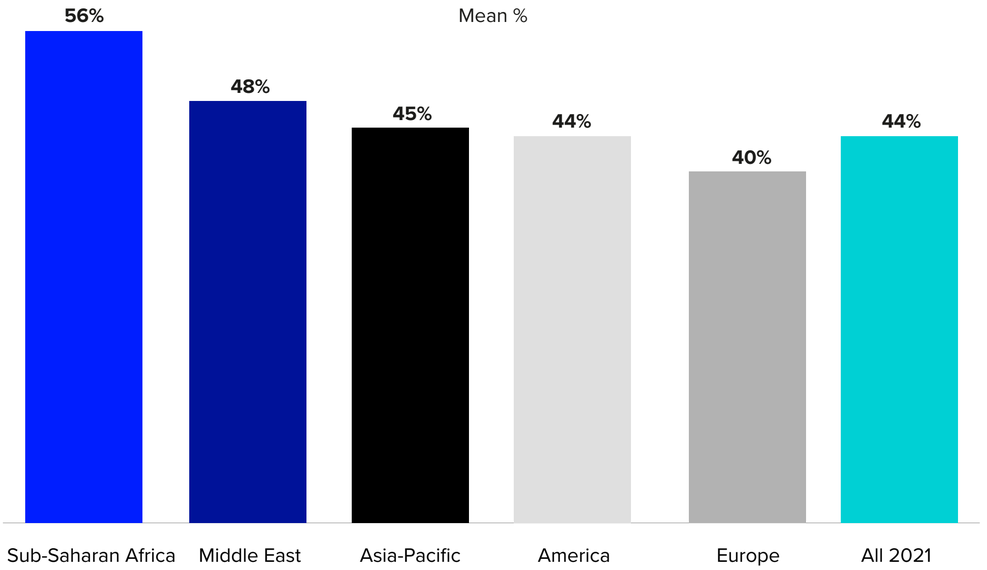


THE REGIONAL PICTURE

While Europe is one of the lowest-performing regions in terms of conducting due diligence checks (40%), the highest-scoring regions are the Middle East (48%) and Sub-Saharan Africa (56%). This may reflect recognition of heightened risks of doing business in these regions, making risk identification and prevention more essential. We have identified other stronger responses from regional respondents compared with our global findings: while 67% of global respondents said they were under pressure to prevent financial crime, this rose to 73% in the Middle East and 80% in Sub-Saharan Africa.

Figure 9: DUE DILIGENCE ON EXTERNAL RELATIONSHIPS REGIONAL COMPARISON

What percentage of these relationships did you conduct any initial formal customer or third-party due diligence check when onboarding them?



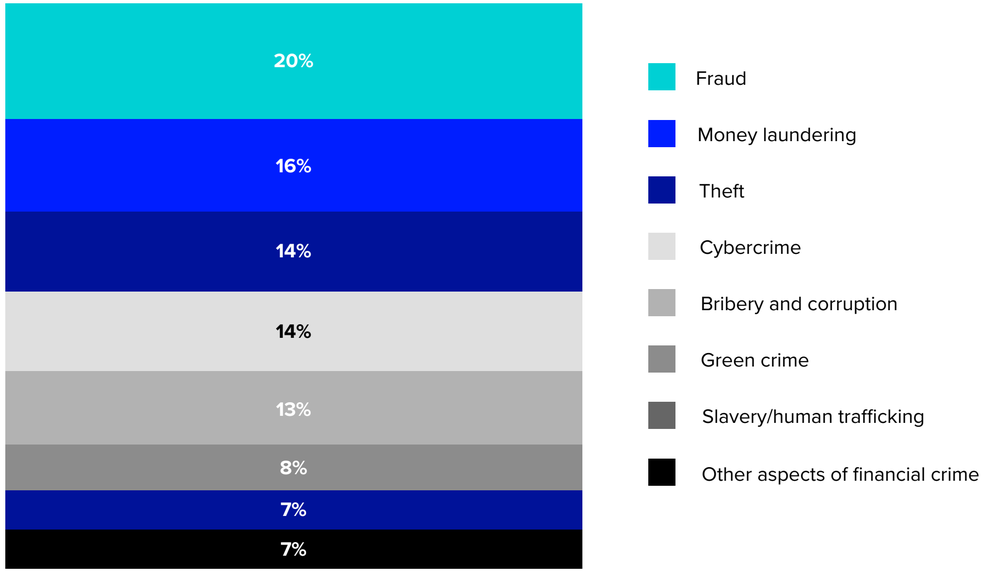
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices, based in America (n=543), Europe (n=1072), Asia Pacific (n=755), Middle East (n=330) and Sub-Saharan Africa (n=220)

FRAUD IS THE KEY FOCUS AREA

Fraud is by some margin the primary area of focus of financial crime prevention, with companies allocating 20% of their overall efforts, time and cost, towards it, compared to 16% for money laundering and 13% for corruption and bribery.

Figure 10: COMPANY EFFORTS TO PREVENT FINANCIAL CRIME

How would you allocate your company's overall efforts (cost and time) to prevent the following aspects of financial crime?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

An LSEG Business

REFINITIV®

Refinitiv® Due Diligence

As a leading global provider of due diligence reports, onboarding workflow, data-based insights, ratings and managed services, we help businesses assess their customers and third parties for any potential risks.

Whatever your business size, location or complexity Refinitiv Due Diligence has the solution, empowering you to make better more informed decisions.

Get in touch today. Refinitiv.com

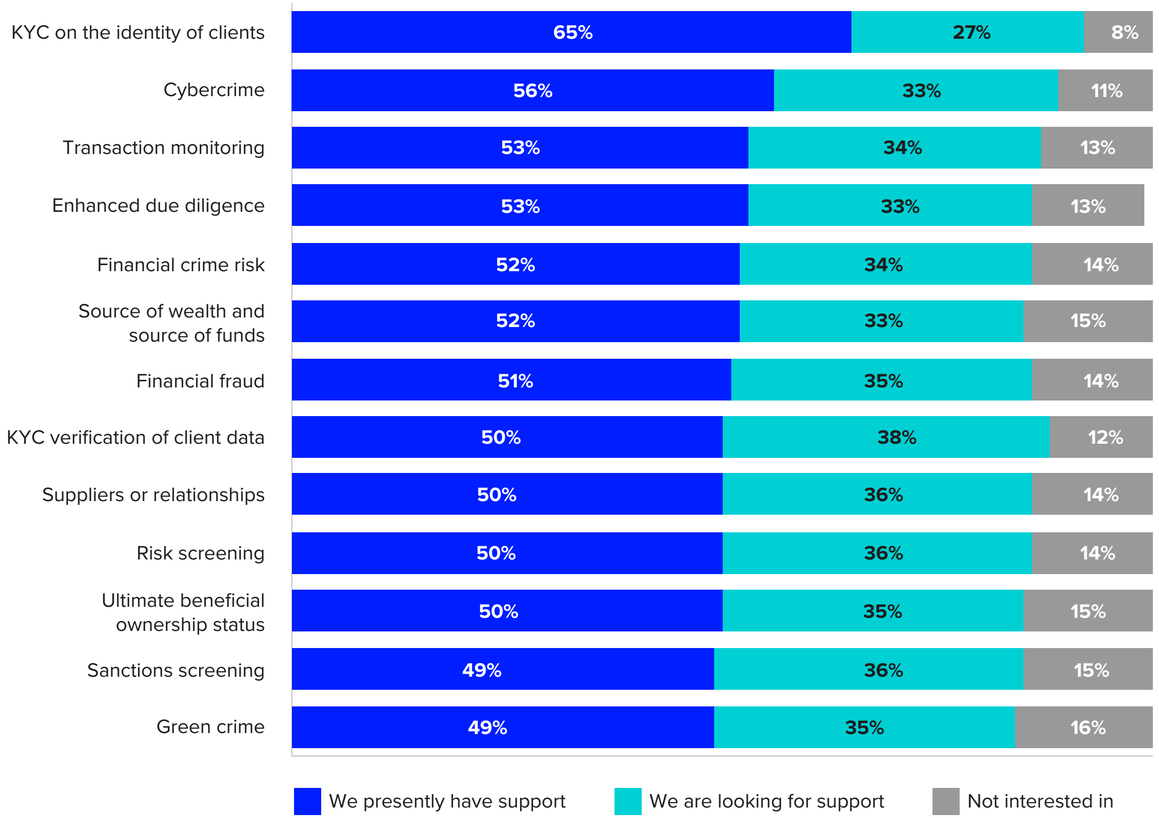
THE REGIONAL PICTURE

The pandemic is increasing the focus on fraud and has made fraud a greater priority for almost half (45%) (Fig. 3) of organisations. Yet there is still plenty of room for improvement: overall, 52% (Fig. 3b) of respondents said that they are not fully managing fraud-related risks.

Technology is a key enabler in the fight against fraud, with 86% (Fig. 11) of respondents either presently using tech to support them with fraud detection or looking to do so in the future.

Figure 11: TECHNOLOGY TO SUPPORT FINANCIAL CRIME PREVENTION

For which of the following are you looking for technologies to support financial crime prevention?



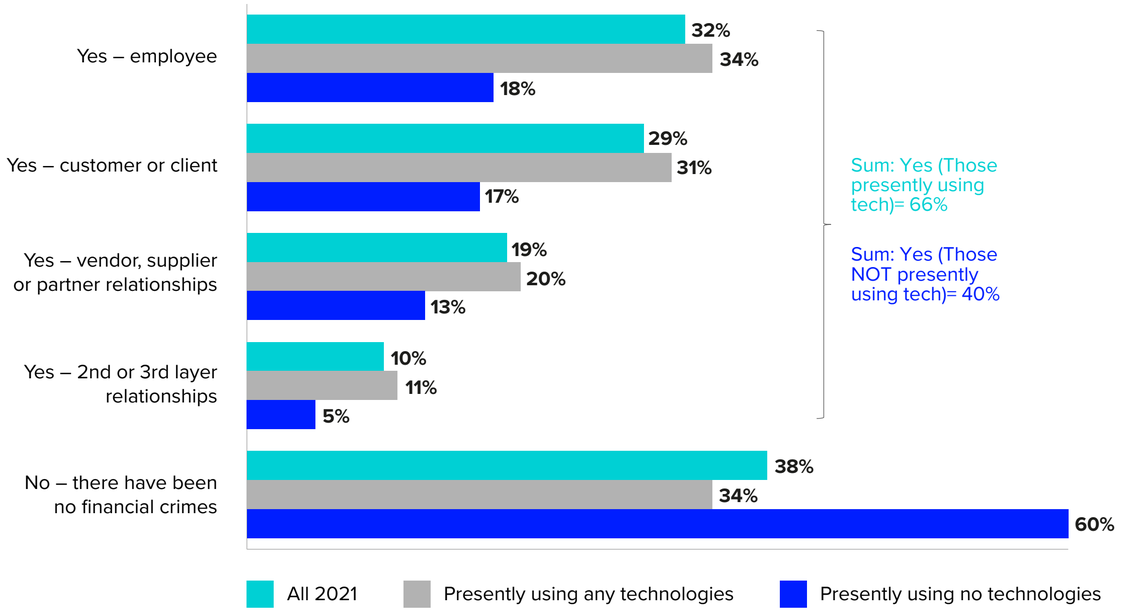
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

CONNECTING AWARENESS AND TECHNOLOGY

Nearly two-thirds (62%) of survey respondents said they were aware of financial crime over the last 12 months, significantly lower than the 73% figure recorded in 2019.

Figure 12: AWARENESS OF FINANCIAL CRIME TECHNOLOGY COMPARISON

Are you aware of any financial crimes (whether they were reported or not) throughout your global operations over the last 12 months (even if inadvertently or through negligence)?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices broken down by those who are presently using technologies for financial crime prevention (n=2531) and those who are not (n=389)

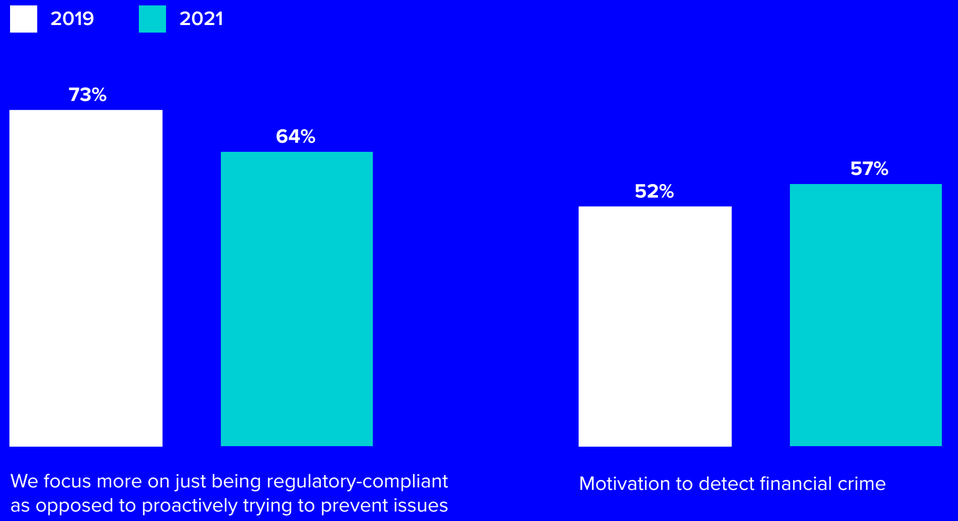
A closer look reveals the direct correlation between financial crime awareness and the use of technology to detect and prevent it. While 66% of tech-savvy respondents were aware of financial crime, this figure fell to 40% for those not using technology to fight financial crime. This suggests that those who do not currently use technology may be less likely to spot financial crime, resulting in a lower awareness of it.

STRONGER MOTIVATION BUT LESS PROACTIVITY

Over half (57%) of the respondents described their motivation to detect financial crime as being 'good or average', five percentage points higher than the 52% recorded in 2019. Yet 64% said they focus more on being regulatory-compliant rather than proactively trying to prevent issues, down from 73% in 2019.

Figure 13: MOTIVATION AND PROACTIVITY TO PREVENT FINANCIAL CRIME 2019 COMPARISON

How strongly do you agree or disagree with the following statements? *How would you rate your company for the following overall?*



Base size 2021 = 2,708 management in large companies across 28 geographies, who are knowledgeable or involved in regulatory compliance and practices

Base size 2019 = 3,138 management in large companies across 28 geographies, who are knowledgeable or involved in regulatory compliance and practices

CONSEQUENCES OF FINANCIAL CRIME

When asked what they consider to be the most harmful consequences of financial crime, corrupting the business environment (33%), encouraging more illegal activity (31%) and the inefficient use of resources (30%) are the highest-ranked categories.

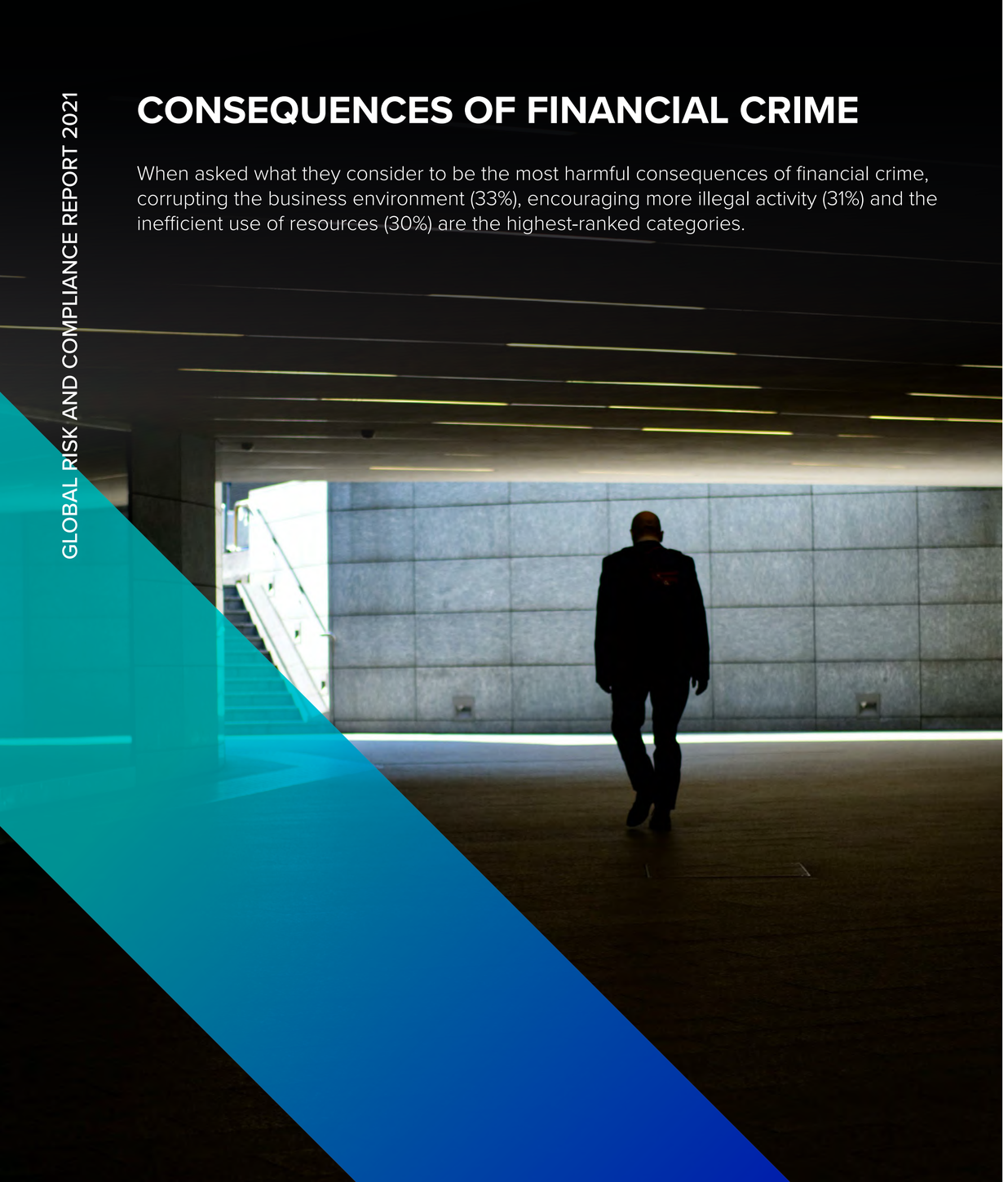
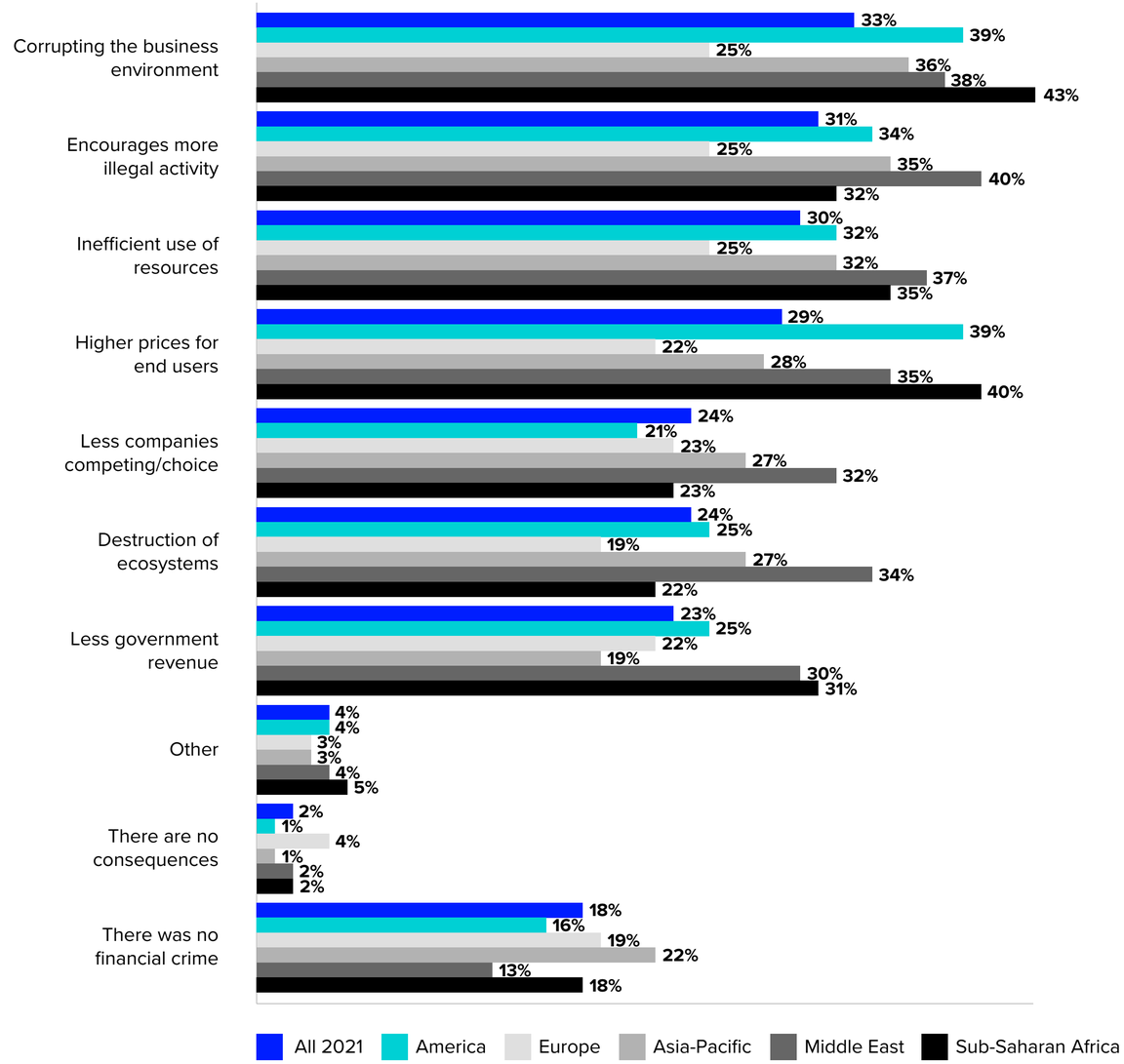


Figure 14: CONSEQUENCES OF CUSTOMER AND THIRD-PARTY RISK REGIONAL COMPARISON

What do you consider are the consequences of this financial crime?

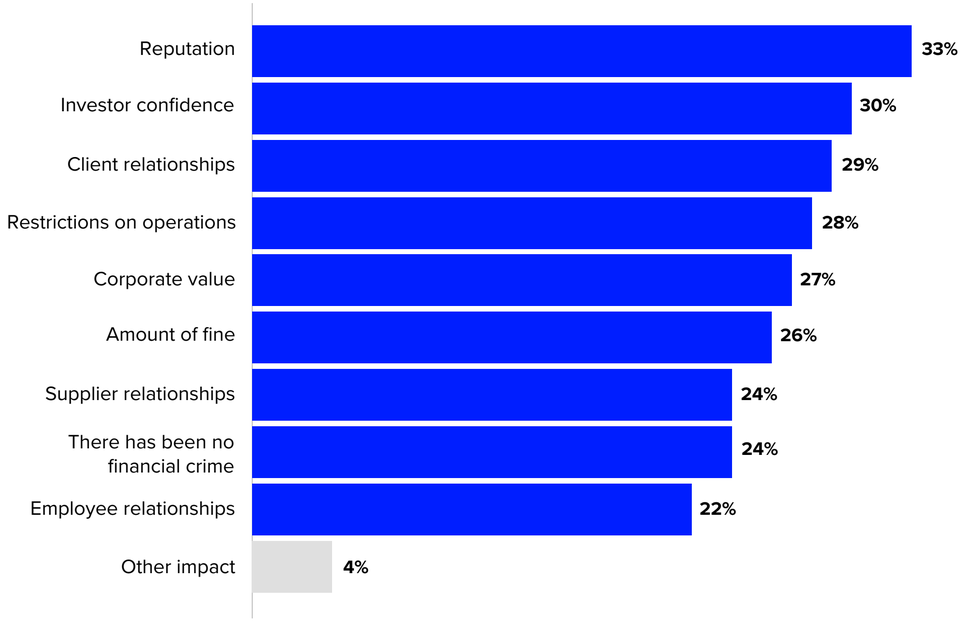


Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices, based in America (n=543), Europe (n=1072), Asia Pacific (n=755), Middle East (n=330) and Sub-Saharan Africa (n=220)

In terms of the impact on the company itself, 33% of respondents said that reputational damage was the number one concern for their organisation.

Figure 15: IMPACT OF BEING ASSOCIATED WITH FINANCIAL CRIME

Which of the following impacts are you concerned about as a consequence of being associated with a financial crime over the last 12 months?

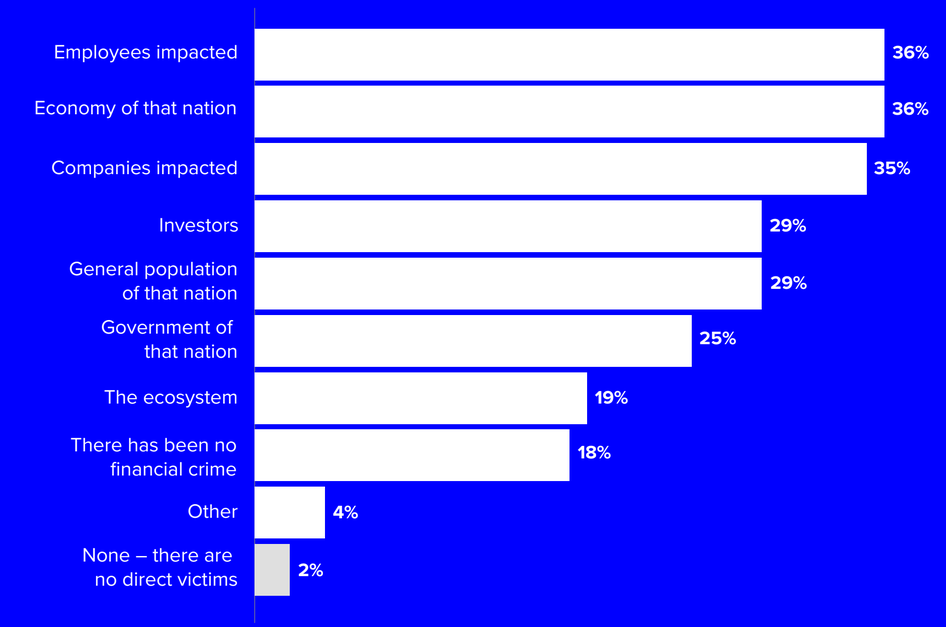


Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

Thinking about who or what respondents considered to be the victims of financial crime, they chose employees (36%), the economy (36%) and the companies (35%) as the most impacted, well ahead of broader concerns about investors (29%) or the general population (29%).

Figure 16: VICTIMS OF FINANCIAL CRIME

Who do you consider are the victims of this financial crime?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

OP-EDS

MAKING GLOBAL VALUE CHAINS MORE RESILIENT THROUGH IMPROVED DIVERSIFICATION AND DUE DILIGENCE

Benjamin Katz, OECD Centre for Responsible Business Conduct

The pandemic has seeded doubts about the ability of global value chains (GVCs) to withstand major disruptions and deliver essential goods and critical materials during crisis conditions. Making GVCs more resilient has therefore become a priority for policymakers.

The OECD's standards on responsible business conduct (RBC) can help policymakers and businesses strengthen GVCs' resilience by reducing the risks of supply chain disruptions and minimising the negative social and environmental impacts of such disruptions. This is reflected in a recent OECD survey of businesses in Latin America and the Caribbean, with 75% indicating RBC practices helped them navigate the pandemic more effectively, and 68% specifically referencing such practices' positive impact on supply chain management as a reason[1].

Similarly, as this report from Refinitiv suggests, the pandemic has accentuated ESG issues' relevance to businesses' operations and decision-making, with two-thirds of respondents (66%) saying that the pandemic increased the importance of ESG to them overall[2].

To home in on how RBC and ESG considerations can help improve 'resilience', let's unpack this term, which can be a catchall for disparate concepts. Its meaning varies in scope: anticipating and mitigating financially material impacts to businesses on the one hand, or impacts on people, planet and society caused by or linked to a business on the other. It can relate to how businesses weather short-term, unexpected crises like the pandemic, or longer-term, foreseeable challenges like climate change.

OECD research on supply chain resilience has shown that supply chains adapted quickly during the pandemic, and that diversifying sources of supply is more effective for enhancing both security and efficiency of supply than reliance on domestic production alone.

But diversifying supply chains necessarily involves sourcing from countries some perceive as risky. As an example, in 2019, the Democratic Republic of the Congo (DRC) produced roughly 70% of the world's cobalt, widely considered a critical mineral (CRM) for its use in battery technologies. Labour-intensive production techniques known as artisanal and small-scale mining (ASM) comprise 15-30% of the DRC's cobalt production, while the rest is industrially produced. Research has linked risks spanning human rights, security contracting and corruption to both industrial and ASM production. But the fact that the DRC is virtually unavoidable as a source of cobalt has led some stakeholders, including many companies, to attempt to parse production into simplistic buckets of "clean" industrial production and "dirty" ASM.

A more sensible approach is to stay engaged across all sources of supply, but to do so responsibly, managing risks where possible and disengaging from suppliers only under very specific circumstances, as for example those circumstances outlined in the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas.

Not only is this approach more suitable for actually improving working conditions for millions of people around the world, it's also good for enhancing resilience by expanding supply and leveraging ASM's role as a swing producer.

Clearly, there is a need for heightened due diligence in these circumstances and as the Refinitiv report demonstrates, modern technology can go some way to addressing this challenge but is not a magic bullet either. Ultimately, the notion of risk-free supply chains is a fiction. The OECD's standards on responsible business conduct enable companies to stay responsibly engaged across a wide spectrum of sources while better anticipating future disruptions. This represents a viable way to build the redundancy and efficiency necessary for more resilient GVCs. It can also contribute to a more just transition to a low-carbon economy in a world likely to remain highly interconnected.

1 Highlights: OECD business survey results on responsible business conduct in Latin America and the Caribbean (forthcoming publication)

2 "RBC" and "ESG" criteria both relate to environmental, social and governance considerations, but RBC risk refers to the risk of adverse impacts to people, society and the environment, not to the company itself. Risk scopes also differ somewhat.

OP-EDS

AI, RISK AND BIAS

Debolina Guha Majumdar, Principal, Data, AI, Automation Advisory Practice, UK & Europe, Infosys Consulting

The two most regulated industries are healthcare and financial services – one manages people's health and the other financial health, enabling the economy of communities and countries. For centuries, banks have been in the business of managing money, providing credit and deciding who is eligible for it. Earlier, the decision or the underwriting part was based solely on human judgement and along with it we have seen a history of discriminatory practices engrained with cognitive bias be it 'redlining' or 'racebased' discriminatory credit provisioning through mortgages to segregate neighborhoods, impede business success or wealth accumulation for people of colour to recent times in 2008 financial crisis when certain subprime predatory loans and products were targeted to minorities. The world has evolved, and technology has made progress in leaps and bounds; It is predicted that AI will contribute >$15 trillion to global economy by 2030. In this age of artificial intelligence (AI), machine learning (ML), big data and digital, machines are in the forefront of transforming financial inclusion, lending and credit allocation to fin crime and green crime. But have we overcome the bias? AI has great potential, but we all need to ensure 'ethical AI' and 'explainable AI' in order to prevent the propagation of those inherent human biases to achieve true diversity and inclusion goals. I believe the five key focus areas in retail banking where ethical AI plays a paramount role in context to bias and risk are:

1. Credit risk and lending
2. Personalisation of product and pricing
3. Know your customer (KYC) and account opening
4. Anti-money Laundering (AML)
5. Environmental, social and governance (ESG) & green crime

43% of those under extreme pressure to increase revenue due to the pandemic said they would like to deploy (AI) and ML to combat financial crime in the future.

Lending and evaluation of credit risk has moved beyond just the usual 'credit scores' to AI, ML looking through a vast array of structured and unstructured data from measuring indebtedness through account balances, financial product holdings to income affordability through rent or mortgage, transactions (do you use public transport, TFL or electric/hybrid cars or buy petrol), subscriptions and finally behavioral and demographic data using them as proxy data such as, postcode address checks (so they know whether you live in a rich or poorer neighborhood), digital footprints, social media data, payments data (do you shop at Waitrose or Asda, what skincare products do you buy) which holistically can show your gender, race, ethnicity, education, economic status (whether you a use a Mac or PC, IOS or Android) and FinTechs are determining interest rates based on all these. Hyper-personalization is the need of the hour. Like retail, FMCG or any other industries, financial services have also pivoted towards deep understanding of customer need and personalize the offerings – product and pricing. KYC is fundamental to account opening and financial inclusion. Gone are the days for huge paper work to open an account, today the FinTechs and challengers banks ensure account opening in three minutes where the customer upload an ID, takes a picture and AI at the back end authenticates with computer vision, intelligent automation and OCR enables real-time verification. A very fine line exists in computer vision how it verifies, accepts or rejects as per race, gender, colour, ethnicity. Trustworthiness and transparency are key to explainable AI (XAI). Whether natural language processing during voice ID verification is biased towards multilingual people and accents. An AI model is as biased as the people who are creating it. The bias percolates from the training historical data that are fed into the system and its views will get reinforced as per the user feedback (people who are testing it). Therefore, we need to be mindful to create diverse teams and bring in diverse thinking to create more fair, transparent systems and inclusive AI, embrace sustainability and stakeholder capitalism, and rebalance purpose and profit to build back better.

Over half (54%) of respondents agreed that Covid-19 had made KYC on the identity of clients a greater priority and 44% said it had impacted the need for KYC verification of client data.

Artificial intelligence and machine learning combined was another common technology type used (45%) to prevent financial crime.

Anti-money Laundering (AML) in banks today heavily relies on not only the business rules and behavioral analytics but also on AI/ML to predict the real cases reducing false positives. AML uses supervised machine learning (learning from historical data and SME knowledge base) and unsupervised machine learning such as hunter model (identifying the strange novel unknowns or outliers in the data). The supervised ML being reliant on historical data and SME knowledge (historically being primarily white males in the western world and the lack of diverse thinking) can lead to racial and gender bias culminating in discrimination against protected classes. The unsupervised model on the other hand lacks explainability to truly justify the outliers that the model is detecting.

43% of respondents said that the pandemic increased the importance of ESG to them overall.

Covid-19 has accelerated the call for a sustainable future and served as a reminder for nations and businesses to rebuild with sustainability management at the heart and core of their corporate strategy. We believe data, AI and analytics can empower financial services organizations in this sustainability journey, embed ESG at the core of business strategy, embrace stakeholder capitalism, and rebalance purpose and profit to build back better. Data is the foundational building block to simplifying the ESG reporting cycle, and transparency in the data is the first step to build a road for better performance. Data management, creating enterprise data hub, data lakes and data governance is also fundamental to ESG management and reporting. This enables trust by capturing traceable, auditable, and consistent data in one secure place for better data quality and assurance. Responsible AI and transparency in data management provides a true picture whether an organization is dumping waste in third world countries, does it have ethical and fair supply chain, is the working conditions and wages fair in the developing world, is the organization declaring accurate gender pay gap and diversity and inclusion ratios etc.

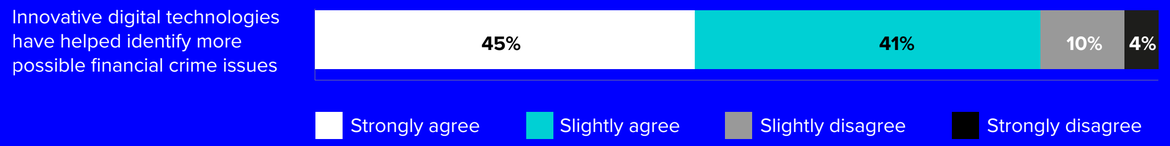
3 | THE PATH AHEAD – TECHNOLOGY LEADS THE WAY

INNOVATIVE TECHNOLOGY AND DATA ARE ALREADY PLAYING A KEY ROLE IN REDUCING RISK – BUT THEY HAVE THE POWER TO RESHAPE IT

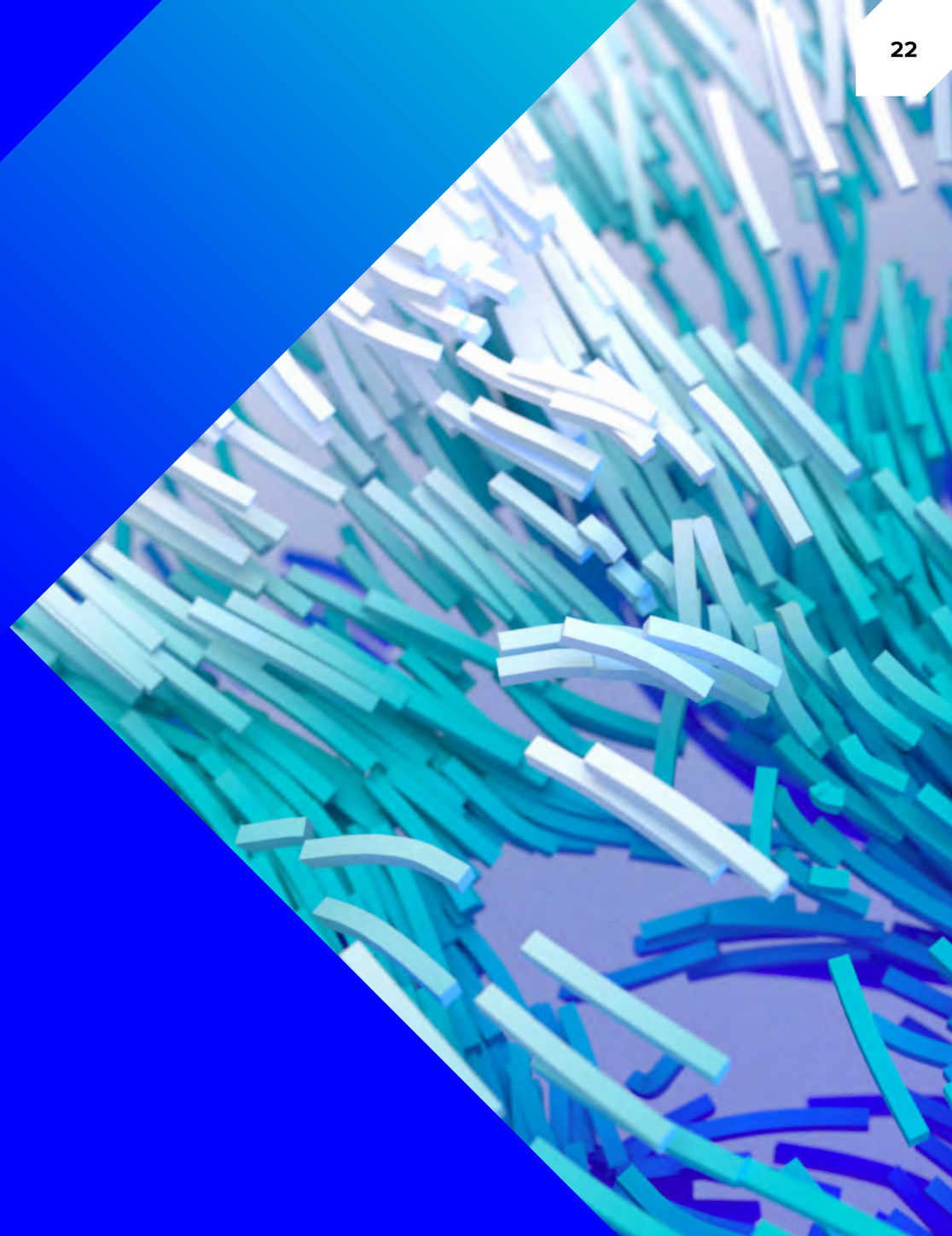
As highlighted in the previous section, the organisations using technology to fight risks associated with financial crime are both more aware of it and more likely to take action. Underscoring the power of technology, 86% of respondents said innovative digital technologies have helped identify financial crime.

Figure 17: DETECTING FINANCIAL CRIME

How strongly do you agree or disagree with the following statement?

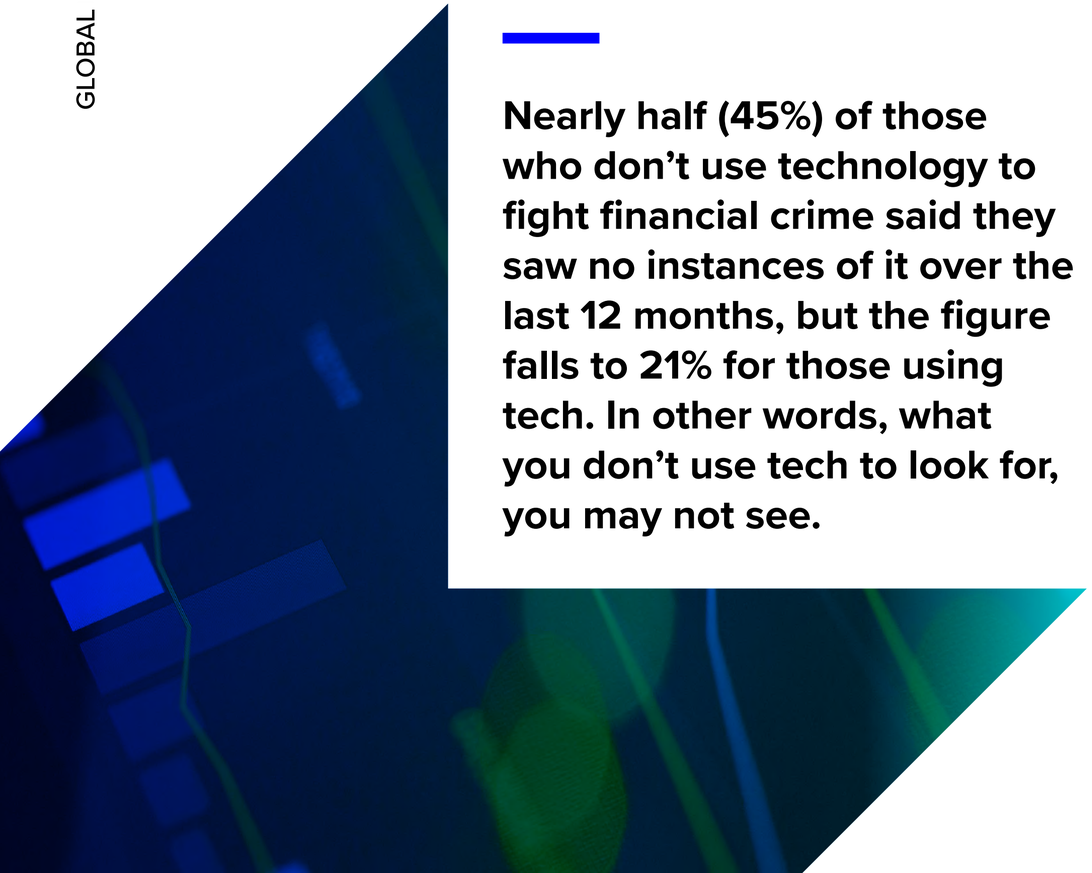


Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices



SEE NO EVIL, HEAR NO EVIL

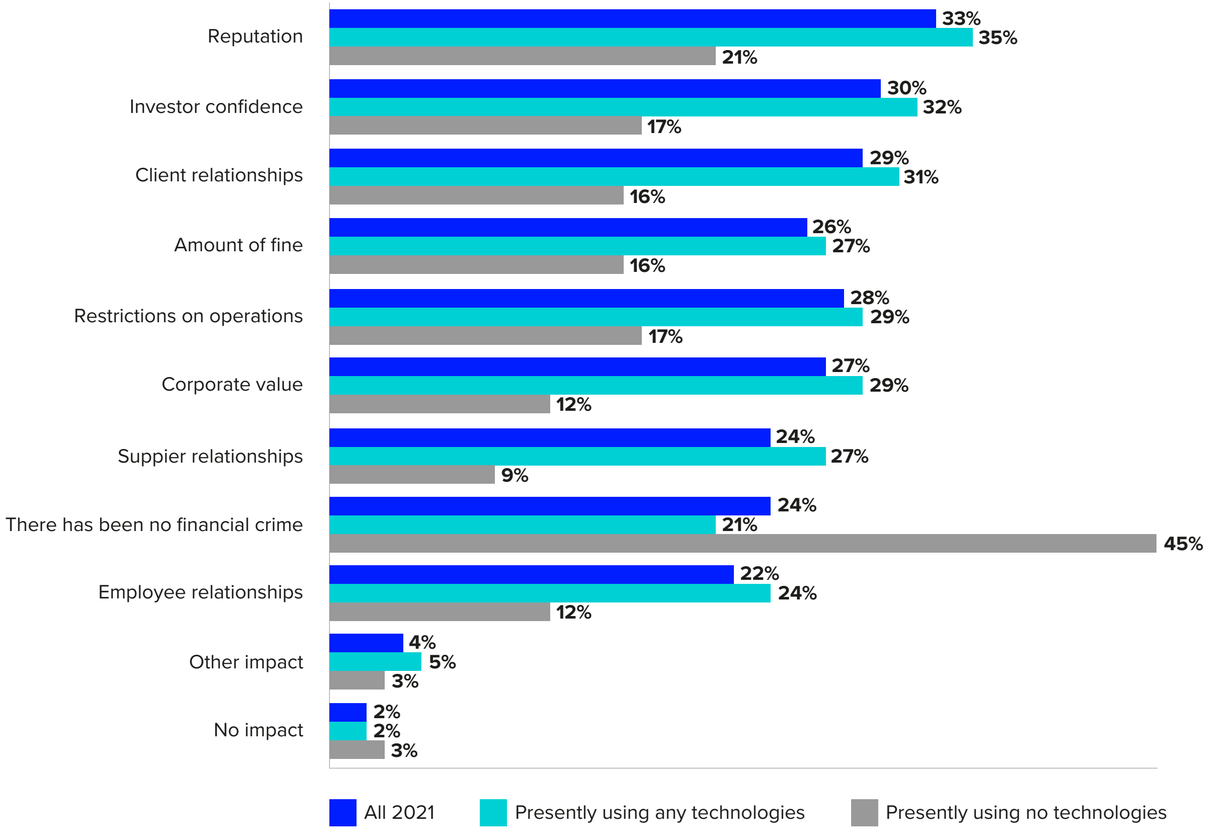
Companies that do not use technology to reduce third-party risks may be unwittingly choosing to operate in ignorance. Not only are they less aware of and less likely to detect financial crime, they are also less concerned about the potential consequences. It is therefore vital for the broader industry to increase engagement, learning and information sharing with these organisations to encourage awareness and investment in appropriate technology.



Nearly half (45%) of those who don't use technology to fight financial crime said they saw no instances of it over the last 12 months, but the figure falls to 21% for those using tech. In other words, what you don't use tech to look for, you may not see.

Figure 18: IMPACT OF BEING ASSOCIATED WITH FINANCIAL CRIME TECHNOLOGY COMPARISON

Which of the following impacts are you concerned about as a consequence of being associated with a financial crime over the last 12 months?



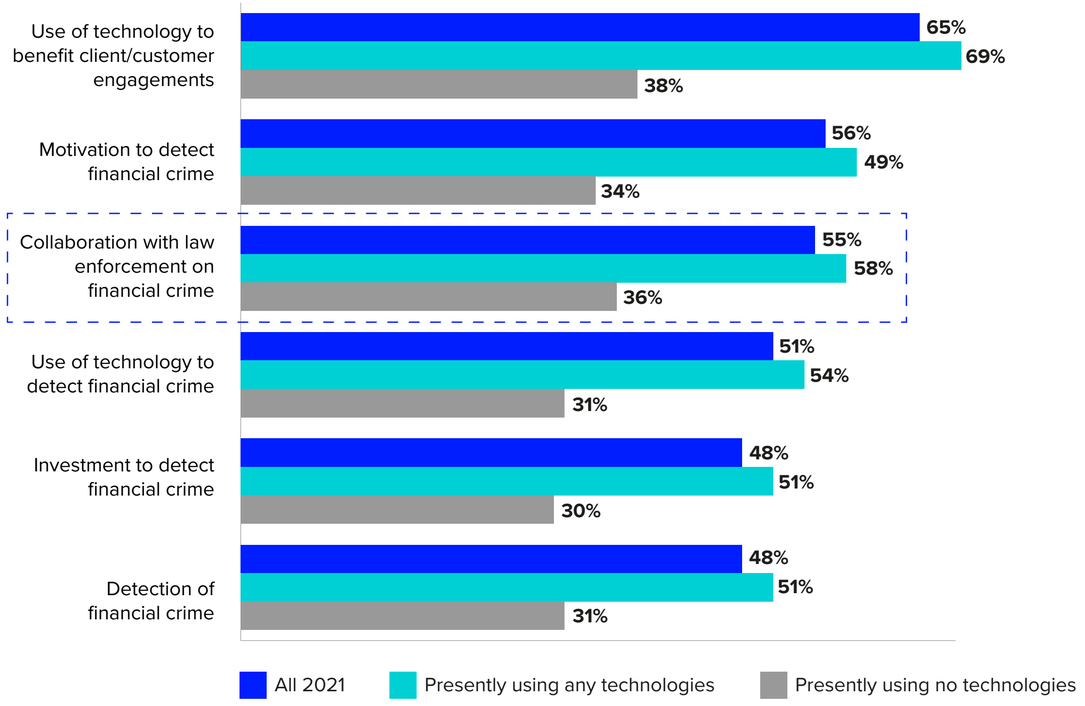
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices broken down by those who are presently using technologies for financial crime prevention (n=2531) and those who are not (n=389)

CONNECTING TECHNOLOGY AND COLLABORATION

It is Refinitiv's view that individuals or organisations acting alone will never successfully combat financial crime, so it is interesting to note the survey's finding said that there is a strong correlation between the use of technology and better collaboration. Those who regularly use technology to prevent risks associated with financial crime are far more likely (58% said they do) to have better collaboration with law enforcement agencies than those who don't (36%).

Figure 19: COMPANY RATINGS TECHNOLOGY COMPARISON

How would you rate your company for the following overall?

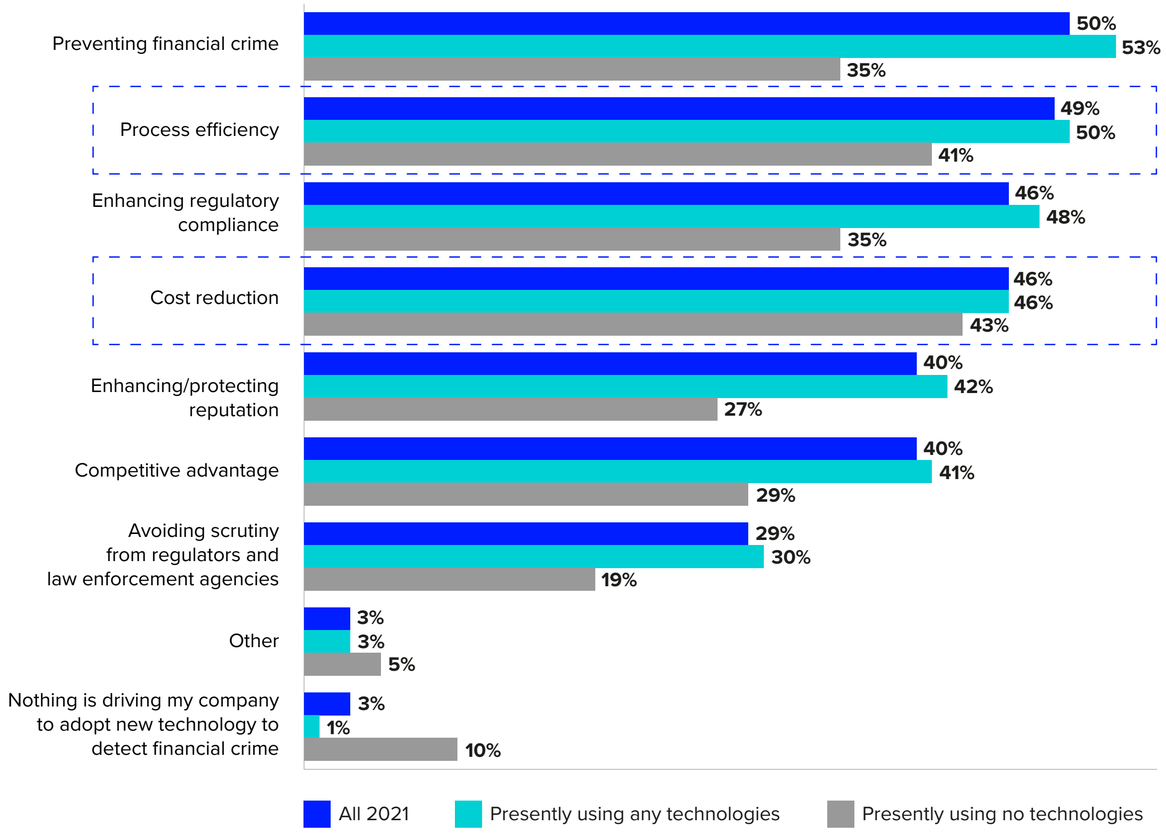


Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices broken down by those who are presently using technologies for financial crime prevention (n=2531) and those who are not (n=389)

Given the advantages of using technology to reduce risk, it is vital to know the factors that inspire adoption: process efficiency (41%) and cost reduction (43%) were the top two triggers for those not yet using tech, well ahead of preventing financial crime (35%). These findings illustrate that the key selling points are commercial pressures.

Figure 20: DRIVERS TO ADOPT NEW TECHNOLOGY TO DETECT FINANCIAL CRIME TECHNOLOGY COMPARISON

What are the drivers encouraging your company to adopt new technology to detect financial crime?



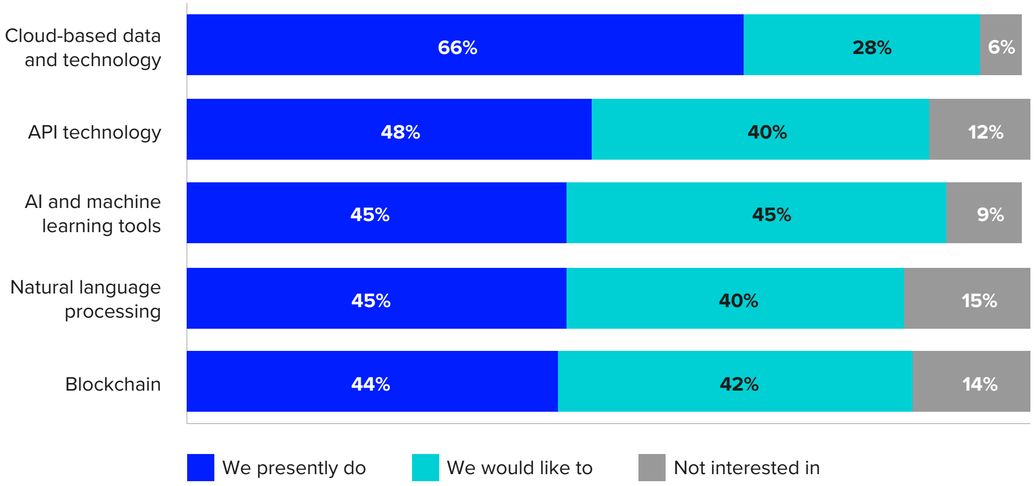
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices broken down by those who are presently using technologies for financial crime prevention (n=2531) and those who are not (n=389)

INVESTING IN TECHNOLOGY AND DATA

Two-thirds of respondents said they use cloud-based data and technology to detect financial crime, while another 28% said they would like to in the future. Artificial intelligence and machine learning combined was another common technology type used (45%) and the greatest aspirational option. This focus on technology reflects our finding from 57% (Fig. 22) of respondents said that automation and digitisation are their key areas of investment.

Figure 21: TECHNOLOGY USED TO PREVENT FINANCIAL CRIME

Which of the following technologies do you presently use for financial crime prevention?



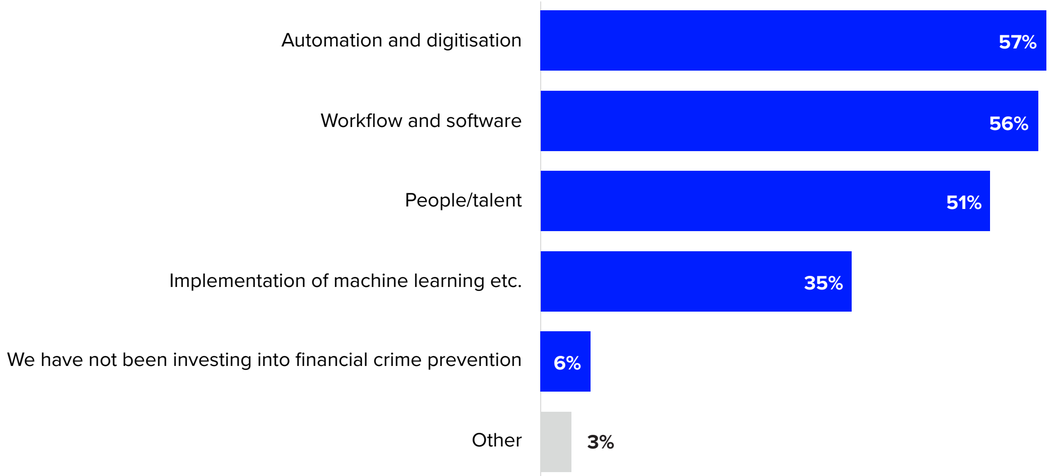
Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

API UPTAKE IS RISING

Fraud detection and anti-money laundering APIs are helping companies to protect their businesses faster and more efficiently by improving integration, interaction and communication. Almost half of respondents (45%) believe that API technology can significantly help with financial crime prevention and uptake looks set to rise significantly. While 48% of respondents already use API tech to prevent financial crime, a further 40% would like to do so in the future.

Figure 22: INVESTING TO PREVENT FINANCIAL CRIME

What key categories of financial crime prevention are seeing the most investment by your company in 2021?



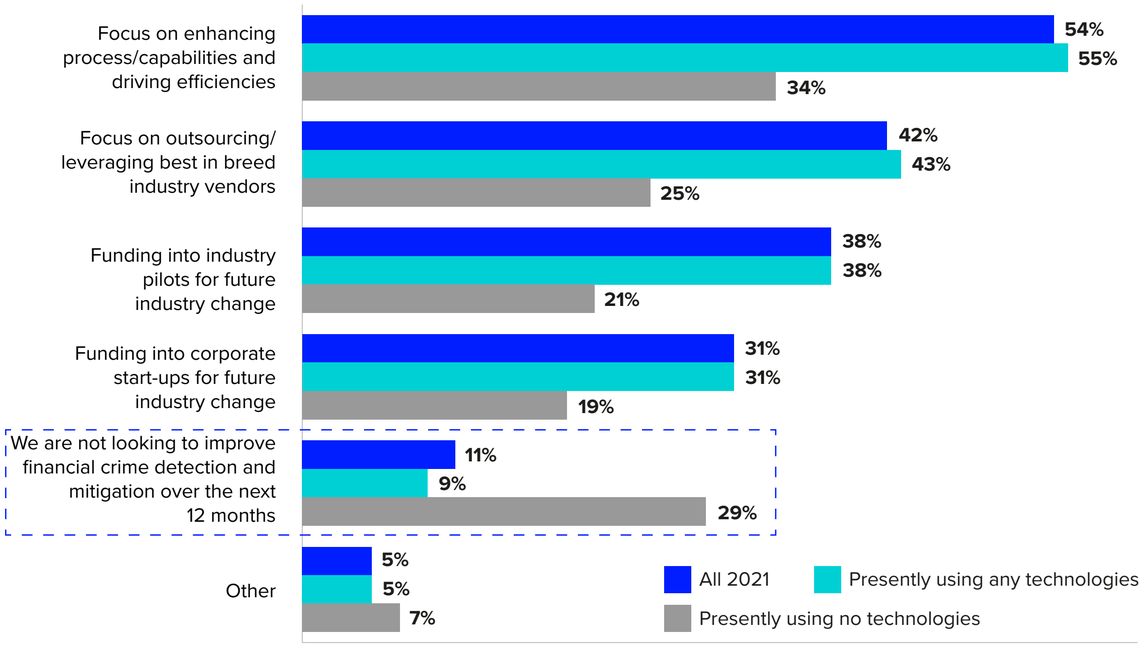
THE MULTIPLIER EFFECT OF INNOVATIVE TECHNLOGIES

The use of technology appears not only to improve current processes but accelerate future adoption: 91% of respondents who use technology in KYC/compliance are looking to improve financial crime detection and mitigation over the next 12 months, versus 71% of those who do not currently use any technology to detect financial crime.

The focus on the future is also reflected in our survey finding that 38% of those using tech said they are likely to fund industry pilots that drive change. But this figure dropped to 21% for those not using tech to fight financial crime.

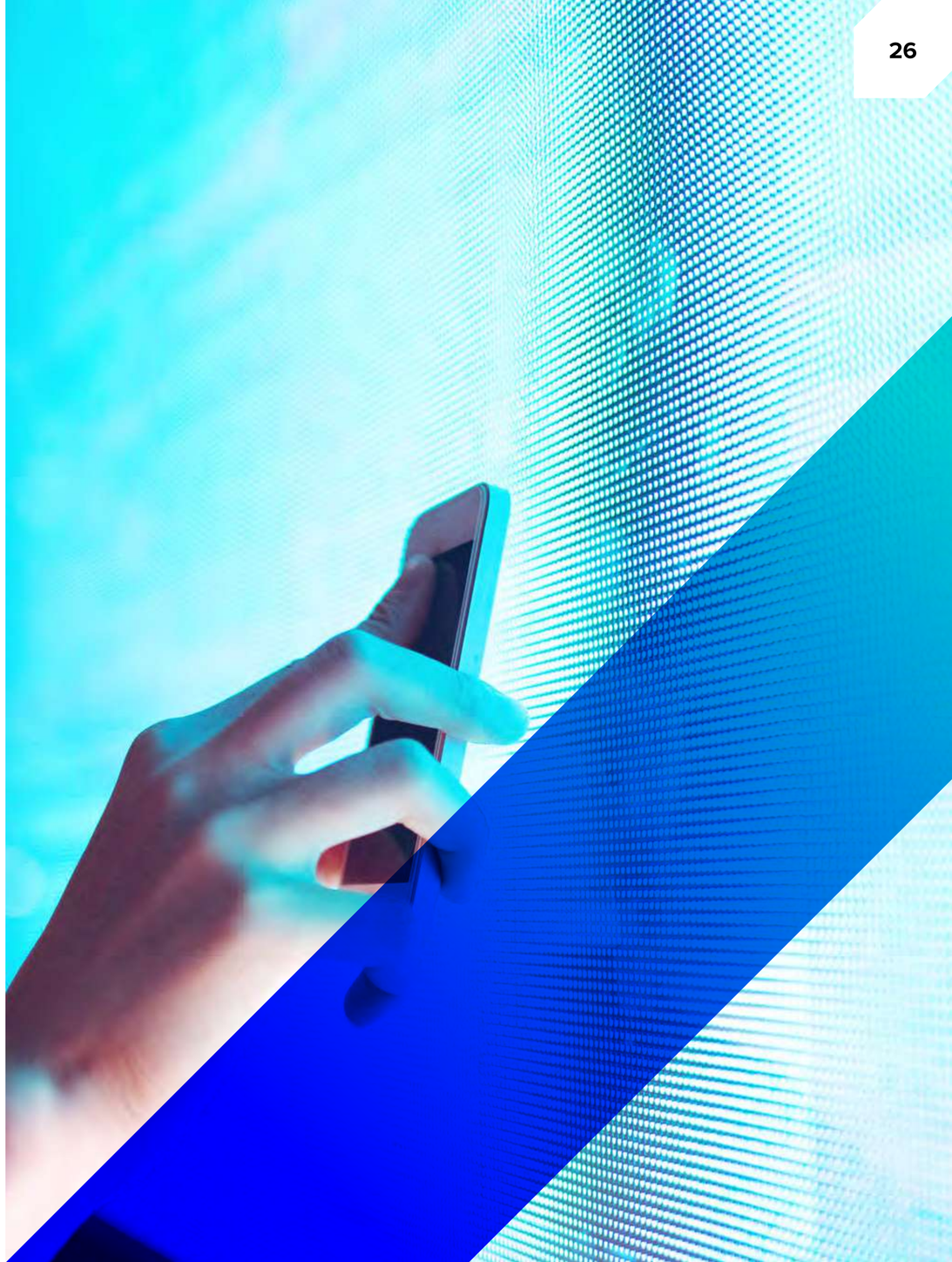
Figure 23: PRIORITIES TO IMPROVE DETECTION – TECHNOLOGY COMPARISON

In order to keep pace with innovation, which of the following best reflects your priorities to improving financial crime detection and mitigation over the next 12 months?



Base size = 2,920 management in large companies across 30 geographies, who are knowledgeable or involved in regulatory compliance and practices

These forward-looking findings suggest that technology adoption can both reduce current risks and drive long-term improvement.



HOW REFINITIV HELPS

We offer solutions that help you meet your customer and third-party regulatory obligations and help prevent reputational damage. Our evolved approach to helping organisations to identify potential risks uses a wide variety of trusted assets and leverages our breadth and expertise to assist clients through the initial onboarding, screening, and due diligence stages to ongoing monitoring and are suitable for any business size, complexity or location and include.

Refinitiv World-Check

Market leading accurate and structured risk intelligence data to help meet your customer and third-party due diligence screening obligations. The data is fully structured, aggregated, and de-duplicated. It can be easily absorbed into various workflow screening platforms in-house, cloud-based, or third-party solutions through a delivery method that suits your requirements. World-Check Risk Intelligence, data used and trusted by the world's biggest companies for over two decades.

Refinitiv Due Diligence

The leading global provider of due diligence reports, onboarding workflow, data-based insights, ratings and managed services. Helping organisations to assess their business relationships for any potential risks and make informed decisions.

Refinitiv Country Risk Ranking

Calculate the location-based risk levels of countries and territories, with detailed, risk-based information on more than 240 countries and territories, categorised by criminal, economic and political factors.

Refinitiv Qual-ID

A digital identity solution that combines ID verification with anti-fraud capabilities of facial matching, document proofing and World-Check risk screening. This integrated set of capabilities helps ensure regulatory compliance, positive client experience and reduced account fraud delivered via one API.

CONCLUSION

Our survey highlights the opportunity that companies have to reduce risk and help to build a safer future

Each year Refinitiv conducts independent surveys looking at different aspects of customer and third-party risk. We have revealed the true cost of financial crime through its impact on companies, society and the environment. More recently we examined how innovation in data and technology can help to identify and disrupt criminal activity. Last year we focused on the hidden risks in supplier, distributor and partner relationships and this year, inevitably, we look at the impact of the Covid-19 pandemic.

Despite the different subjects, we are all too often telling essentially the same story: even with stronger regulation, more powerful enforcement actions and greater investment by companies, we still find that many organisations are not carrying out all the processes needed to identify and mitigate risks.

CHANGING THE STORY

Although the risk picture has once again worsened, with the proportion of organisations carrying out due diligence on third parties falling from 49% in 2019 to 44% in 2021, the situation is different. The pandemic has raised risk levels, but it has also accelerated technology adoption, increased collaboration and intensified the focus on addressing longstanding problems: 86% of respondents agreed that innovative digital technologies have helped identify financial crime and 57% are investing in automation and digitisation during 2021.

WORKING TOGETHER

So, we conclude our 2021 report by highlighting that, having encountered heightened risks as a result of the global pandemic, organisations can and must seize the opportunities offered by technology to address them. As a leading provider of data and compliance technology, we have a key role to play in helping organisations rise to this challenge, supporting digital transformation in risk management and satisfying the growing need for trusted data. We embrace that challenge and look forward to working with our customers, regulators and industries across the world to reshape risk and build a safer future.

Join the conversation #FightFinancialCrime and #FightGreenCrime

READ MORE FROM OUR RISK AND COMPLIANCE SERIES

Edition 1 | Global Report

The true cost of financial crime

Understand the true cost of financial crime and its impact – not just on companies and governments, but also the human victims exploited by criminal gangs which launder their gains through the financial system.

Read more

White Paper

Global sustainable development

Discover how green crime, which is closely linked to corruption, organised crime and money laundering, can be mitigated through use of supply chain risk tools, ESG data and greater collaboration.

Read more

Edition 2 | Global Report

Innovation and the fight against financial crime

Discover the latest innovations – revealing how emerging technologies, trusted data and new collaborations are helping to turn the tide against financial crime.

Read more

Edition 3 | Global Report

Hidden threats within third-party relationships

Understand the substantial impact Covid-19 had on the risk landscape, particularly in terms of supply chain and third-party risk, but also why green crime and environmental risks are rising.

Read more

Visit **refinitiv.com** | @Refinitiv Refinitiv

Refinitiv, an LSEG (London Stock Exchange Group) business, is one of the world's largest providers of financial markets data and infrastructure. With $6.25 billion in revenue, over 40,000 customers and 400,000 end users across 190 countries, Refinitiv is powering participants across the global financial marketplace. We provide information, insights and technology that enable customers to execute critical investing, trading and risk decisions with confidence. By combining a unique open platform with best-in-class data and expertise, we connect people to choice and opportunity – driving performance, innovation and growth for our customers and partners.

REFINITIV®

An LSEG Business

RE137410/7-21