


---

# THE REAL RISKS: HIDDEN THREATS WITHIN THIRD-PARTY RELATIONSHIPS







# World-Check®

Uncover risk. Take action.

A powerful combination of data, technology  
and trusted human expertise to help:

- Simplify and accelerate risk screening
- Meet regulatory obligations
- Protect against financial crime risk

[refinitiv.com/world-check](https://refinitiv.com/world-check)

**REFINITIV®**  
DATA IS JUST  
THE BEGINNING®





# FOREWORD



**Phil Cotter**  
Managing Director,  
Risk Business,  
Refinitiv

Our survey highlights how, in an increasingly interconnected and globalized world, many third-party risks are going undetected.

In recent years Refinitiv has carried out independent surveys looking at the true cost of financial crime, revealing its impact on companies, governments, society and the environment. More recently we have examined how innovation in data and technology can help to identify and disrupt criminal activity.

This year we focus on the critical area of third-party relationships, revealing the hidden risks in supplier, distributor and partner relationships.

This is a timely report, with the COVID-19 pandemic applying huge stress to global supply chains and allowing criminals to exploit the pandemic to defraud companies and government agencies. It also corresponds with the recent announcement by European Commissioner for Justice, Didier Reynders, of the EU's commitment to introduce rules for mandatory corporate environmental and human rights due diligence.

Against this background, organizations face greater regulation and stricter enforcement actions. In 2019,

companies received penalties totaling US\$2.9 billion under the US Foreign Corrupt Practices Act (FCPA), with several officers and directors of those companies being found individually liable for breaches.

It is clear from our report that many companies today are not doing enough to protect themselves against the risk of involvement in criminal activity and resulting regulatory enforcement, with the survey revealing that 43% of third-party relationships are not subject to any form of due diligence. With an increasing focus from regulators on sanctions, corruption, sustainability and human rights, companies clearly need to upgrade their risk management procedures and capabilities. But how can they rise to this challenge? What is stopping them and what can be done to support them?

Our in-depth analysis seeks to find answers. With respondents citing a lack of data as the biggest challenge in identifying supply chain risk, Refinitiv has a central role in providing the trusted data and innovative technology to assist organizations with the effective and efficient management of third-party risk.

We also conducted and include interviews with leading NGOs (RUSI, Ethical Systems, United for Wildlife) and INTERPOL to examine the wider economic, social and human impact.

Finally, we identify ways in which business, governments and Refinitiv are working together to help organizations to better identify and manage third-party risk.

**Join the conversation #FightFinancialCrime**





# ABOUT THE REPORT

This report is based on research commissioned by Refinitiv that was conducted online by an independent consulting company in February 2020. Nearly 1,800 global third-party relationship, risk management and compliance professionals in corporate organizations completed the survey.

This research was conducted across 16 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%.

Within this report, we also refer to the results of an additional Refinitiv survey that was conducted in February 2020. This separate survey gathered the opinions of 250 global institutional investors representing a total of over US\$10 trillion of assets under management.

TOTAL	USA*	Brazil*	China*	India*
1794	110	105	108	107

Australia*	United Kingdom*	Germany*	France*	Singapore*
107	128	108	108	104

Spain	Hong Kong	South Africa	Russia	Saudi Arabia	The Netherlands	Canada
110	110	120	119	130	110	110

\*Countries surveyed in 2016 will be referred to as ‘trended countries’ throughout the remainder of this report

## Size

Large 899      SME 895

## 17.5m

The 1,800 survey respondents worked for organizations with a total of over 17m third-party relationships



# DEFINITION

For the purpose of this report we have defined a ‘third-party’ as any person or organization that is connected to a supply chain or is executing business on an organization’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.

# HIGHLIGHTS

## THE REAL PICTURE

With an average of nearly 10,000 third-party relationships to deal with, many organizations are not completing full third-party due diligence at either onboarding or ongoing monitoring stages. This is compounded by competitive pressures, greater globalization and increasingly complex supply chains.

- 43%** of third parties are not subject to due diligence checks, according to our survey respondents. This is six percentage points higher than when comparing the results for the same countries in our 2016 survey
- 60%** of respondents are not fully monitoring third parties for ongoing risks
- 63%** of respondents agree that the economic climate is encouraging organizations to take regulatory risks in order to win new business
- 53%** of respondents say that they would report a third-party breach internally and only 16% would report it externally

## DRIVERS AND BLOCKERS

Despite greater regulation and stronger enforcement action, organizations are struggling to gain visibility of all third-party risks to enable appropriate action to be taken. Green and environmental crime risks are rising but require more accurate analysis.

- 61%** say that prosecution would be unlikely if they breached third-party related regulations
- 25%** of an organization's corporate value would be lost as a result of a regulatory breach, according to our survey respondents
- 50%** say they know of an enforcement action being taken against their company in relation to a third-party risk

## TAKING ACTION

Better data, greater innovation and new forms of collaboration hold the key to reducing third-party risk. Building greater transparency and resilience into supply chains is also crucial.

- 37%** of respondents believe that a lack of data is a problem they face in identifying risks within their supply chain
- 93%** say that spending increased after an enforcement action related to third-party risk
- 62%** of respondents do not know how many third parties they engage are outsourcing work to others



# 1 | THE REAL PICTURE

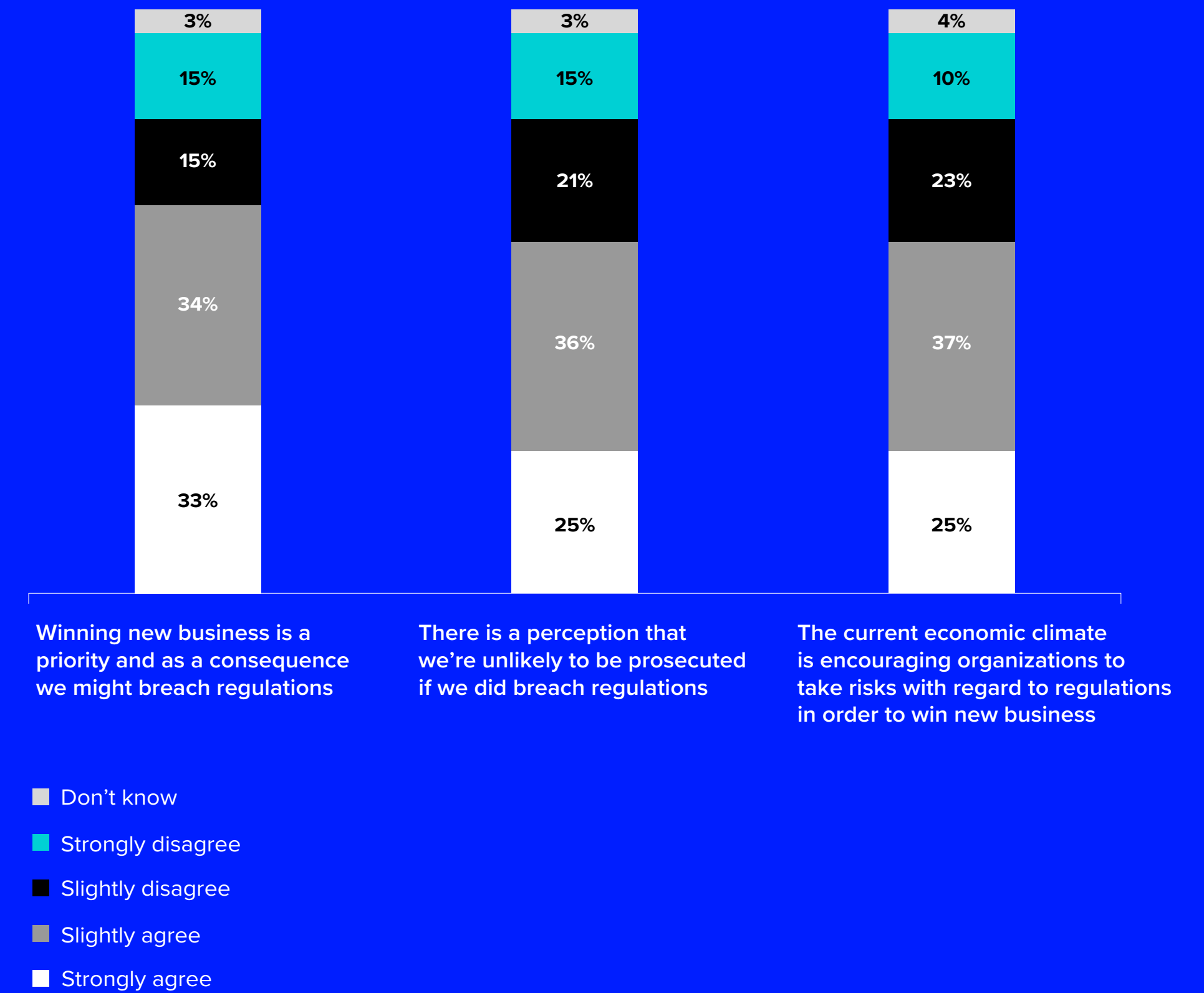
## RISK EXPOSURE IS INCREASING BUT DUE DILIGENCE IS NOT KEEPING PACE

### Setting the scene

To understand the full picture, first we need to consider the background. Organizations have a high volume of third-party relationships across their global operations, with our survey revealing that the average number is 9,735. The benefits of such arrangements can outweigh the risks (Fig. 1.1), with nearly two-thirds (63%) of respondents agreeing that the economic climate is encouraging organizations to take regulatory risks in order to win new business. The imperative for this is clear, with 74% saying that third-party relationships have allowed their company to be more flexible and competitive.

Figure 1.1: Level of agreement with key statements

What is your level of agreement with the following key statements?



## SCREENING SHORTFALL

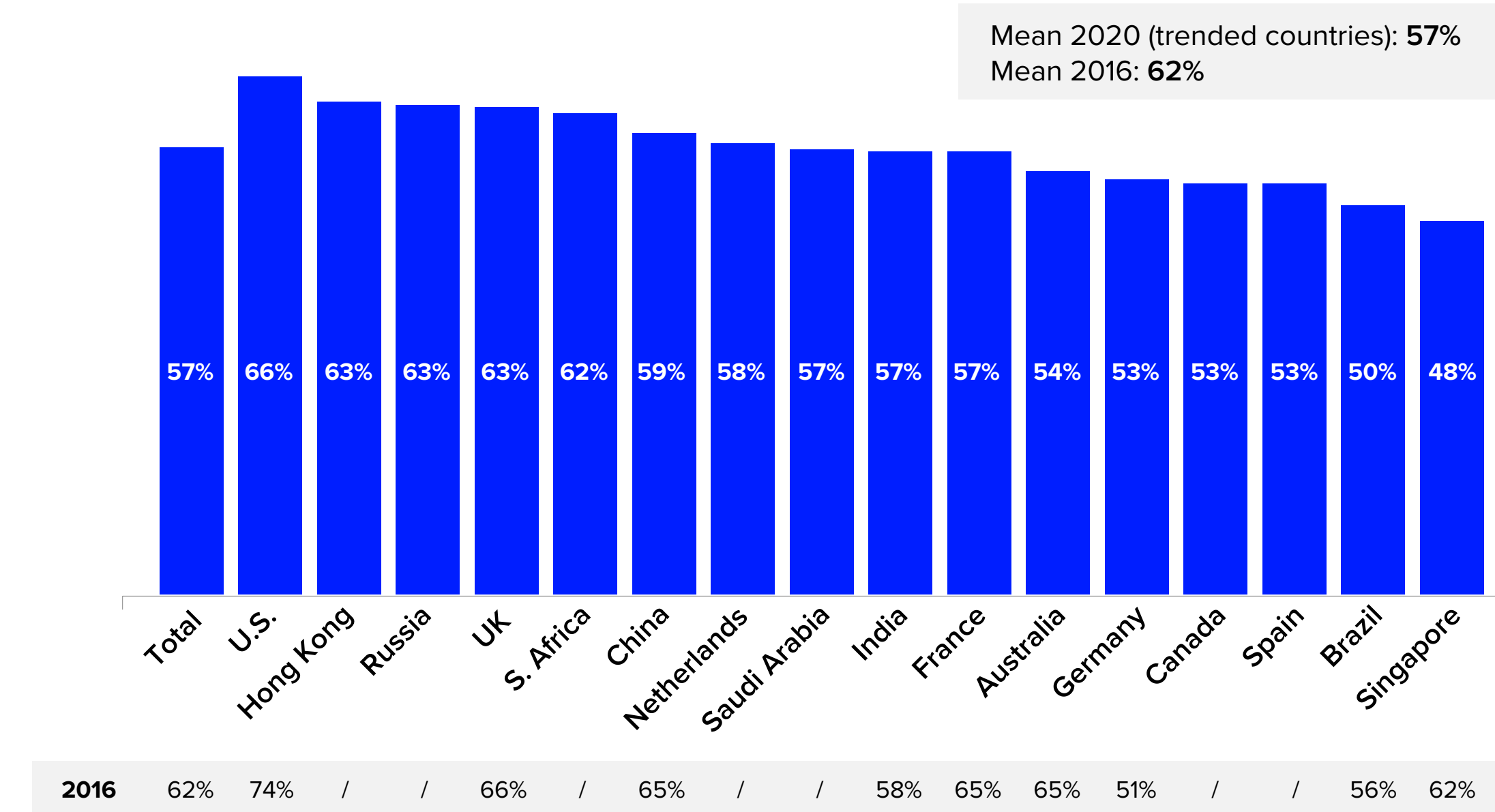
The factors previously mentioned contribute to our key survey finding (see Fig. 1.2) that, on average, 43% of third parties are not subject to due diligence checks by our respondents. This is six percentage points higher than when comparing the same countries in our 2016 survey.

Over the same period, the average number of third-party relationships has increased by 3%, suggesting that organizations are struggling to maintain standards while dealing with the greater volume and complexity of relationships in an increasingly interconnected world.

From a regional perspective (Fig 1.2), set against the global average of just 57% of third parties undergoing due diligence, the U.S. was the strongest performer with 66% and Singapore brought up the rear with 48%. In terms of industries, automobile parts/industrial engineering (60%), TMT (60%) and financial services (60%) led the way, while industrials (54%), construction (53%) and healthcare (50%) were the worst performers in terms of due diligence. The latter figure is of particular concern in light of the COVID-19 pandemic, with the extraordinary demand for medicines and medical equipment creating an environment in which fraudsters can flourish. Looking at the results in relation to company size, the global figure for due diligence was 61% for large corporations compared to 54% for SMEs.

Figure 1.2: Percentage of due diligence on third parties

Approximately what percentage of your third parties has your organization conducted due diligence on? (Please select one response)



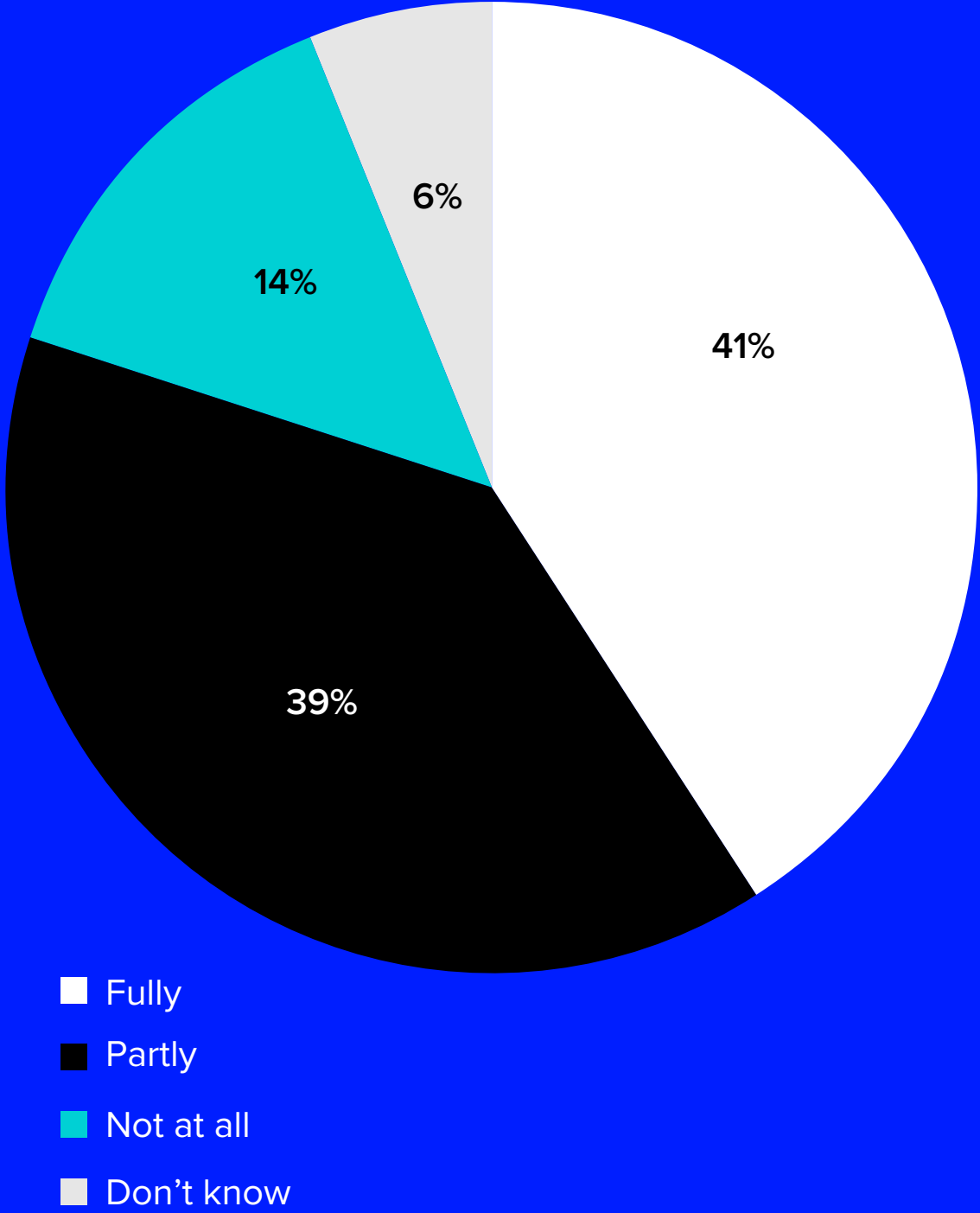


# ONGOING MONITORING

It is vital to conduct due diligence, not only during onboarding but also to regularly revisit and review risk levels. Yet 60% of respondents say they are not fully monitoring third parties for ongoing risks (Fig. 1.3), which does represent a small improvement of four percentage points when comparing the results for the same countries in our 2016 survey.

Figure 1.3: Management risk with third parties

What steps does your company current take in regards to managing the third-party onboarding process?



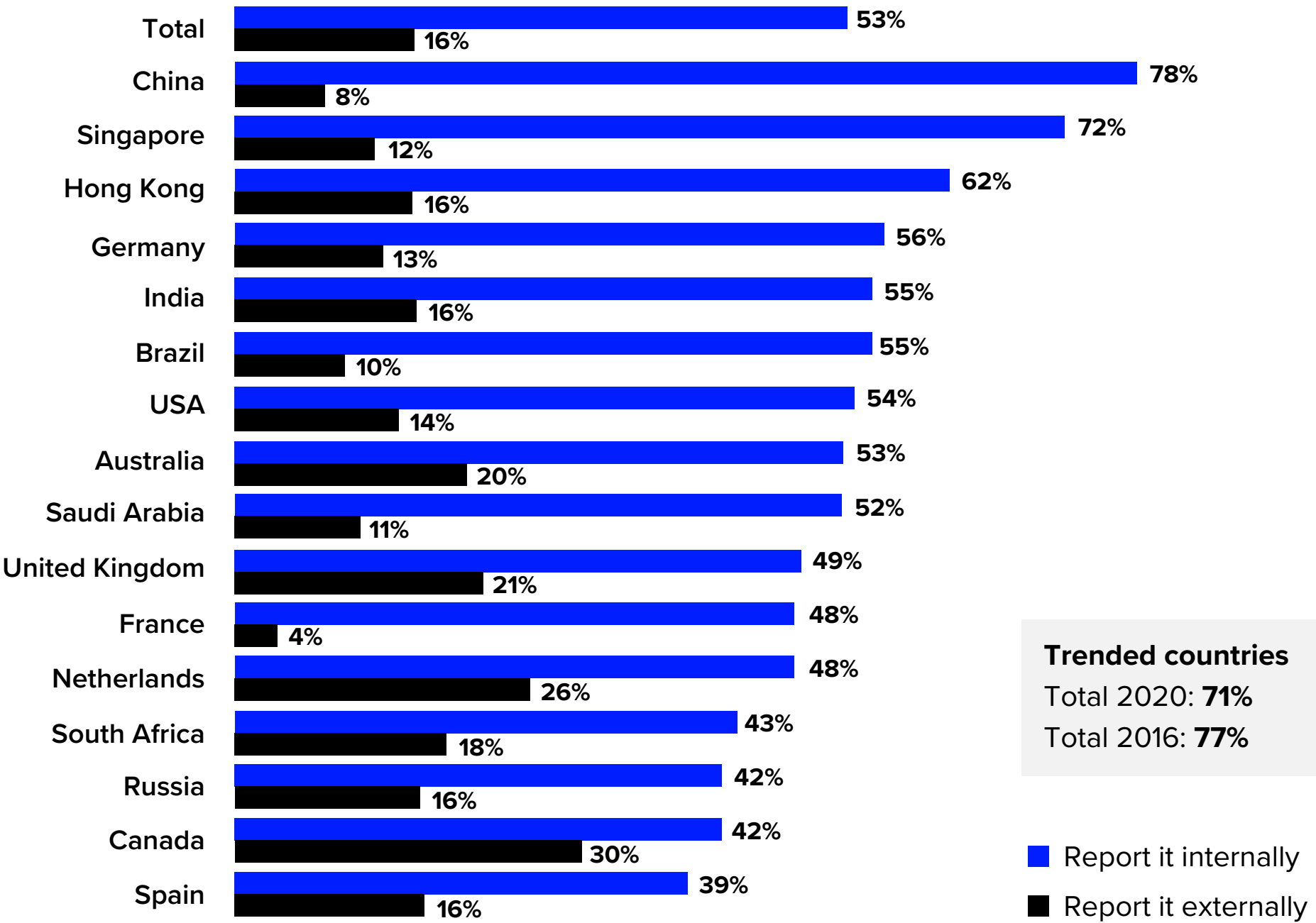
# REPORTING BREACHES

Risks can only be fully understood by organizations, industries and their regulators if breaches are reported. Yet our survey reveals that only 53% of respondents would report a third-party breach internally and only 16% would report it externally.

From a regional perspective (Fig. 1.4), those in China are most likely (78%) to report a breach internally but are among the least likely (8%) to do so externally. Canada tops the survey for reporting breaches externally (30%), while France is lowest with 4%. In terms of sectors, Retail leads the way with 24% of respondents claiming to report breaches externally while the professional services industry is the least likely at just 12%.

Figure 1.4: Likelihood to report if a third-party is caught breaching regulation, by country

If you came across a third party you're working with that breached regulations, what would you most likely do? (Please select one response)



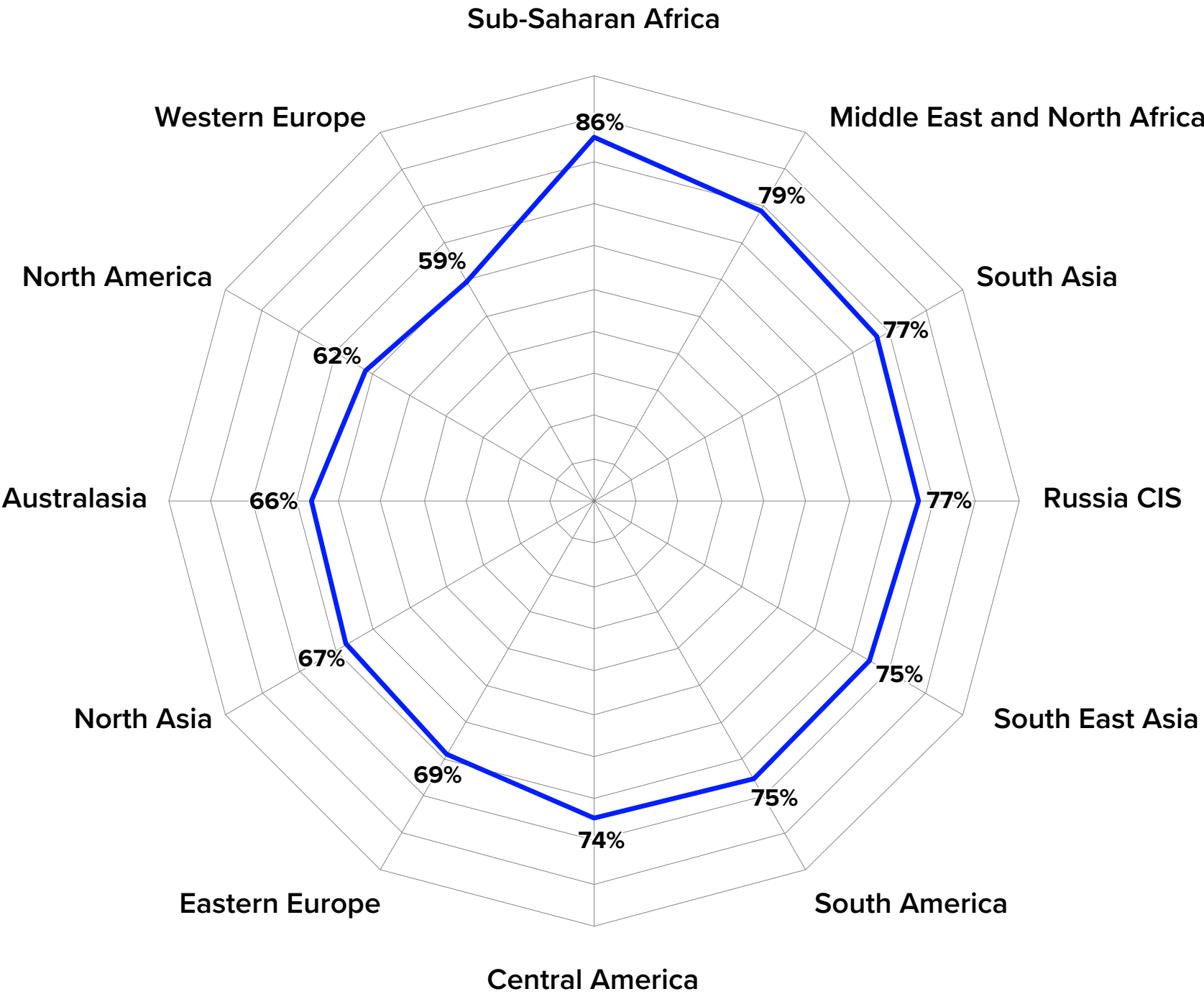


# REGIONAL RISK LEVELS

Sub-Saharan Africa has the highest level of third-party risk (as shown in Fig. 1.5), according to all survey respondents, with 45% of respondents classing it as high risk. This seems to match the reality, as it was also rated high risk by 46% of those with third-party relationships in the region. Australasia (20%) and Western Europe (20%) were rated the least risky, just ahead of North America (22%) and Eastern Europe (22%). Generally, large companies considered all regions less risky than their SME counterparts. The biggest exception to this was for Russia CIS, where 28% of SMEs considered it a low-risk region, compared to only 19% of large enterprises.

Figure 1.5: Risk levels in third-party regions

How would you generally rate the risk level of having third-party relationships in each of the following regions? Sum: high/medium risk



Proportion of respondents who consider these regions high/medium risk





## 2 | DRIVERS AND BLOCKERS

### GREATER REGULATION AND STRICTER ENFORCEMENT ACTIONS ARE NOT HAVING THE DESIRED EFFECT

#### Regulation is a deterrent, but not always feared

Organizations are operating in a more highly regulated environment today than they were during our 2016 survey. This can be illustrated by the fact that companies received penalties totaling US\$2.9 billion in 2019 under The Foreign Corrupt Practices Act (Fig. 2.1).

Figure 2.1: Foreign Corrupt Practices Act Enforcement Actions

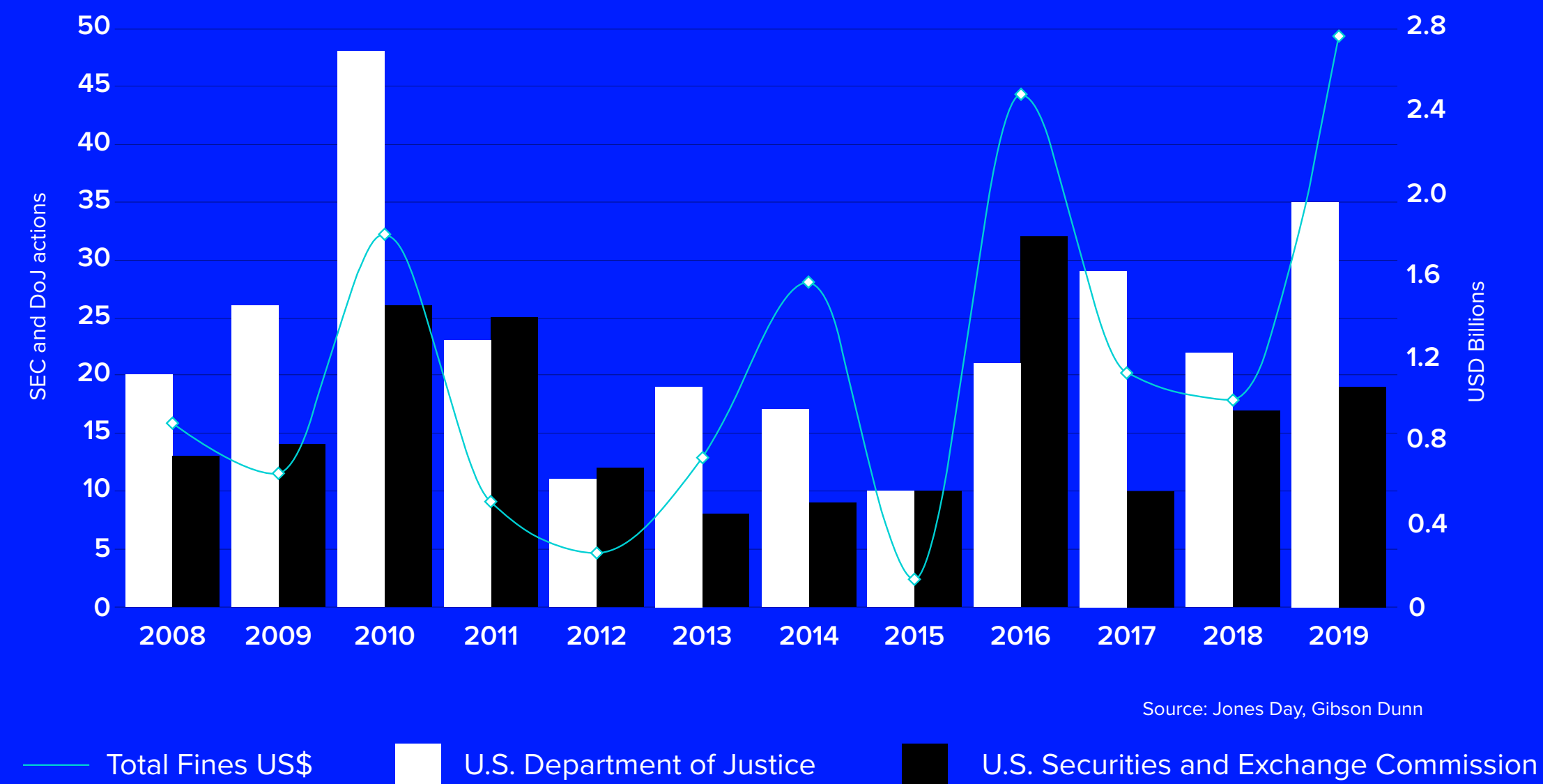
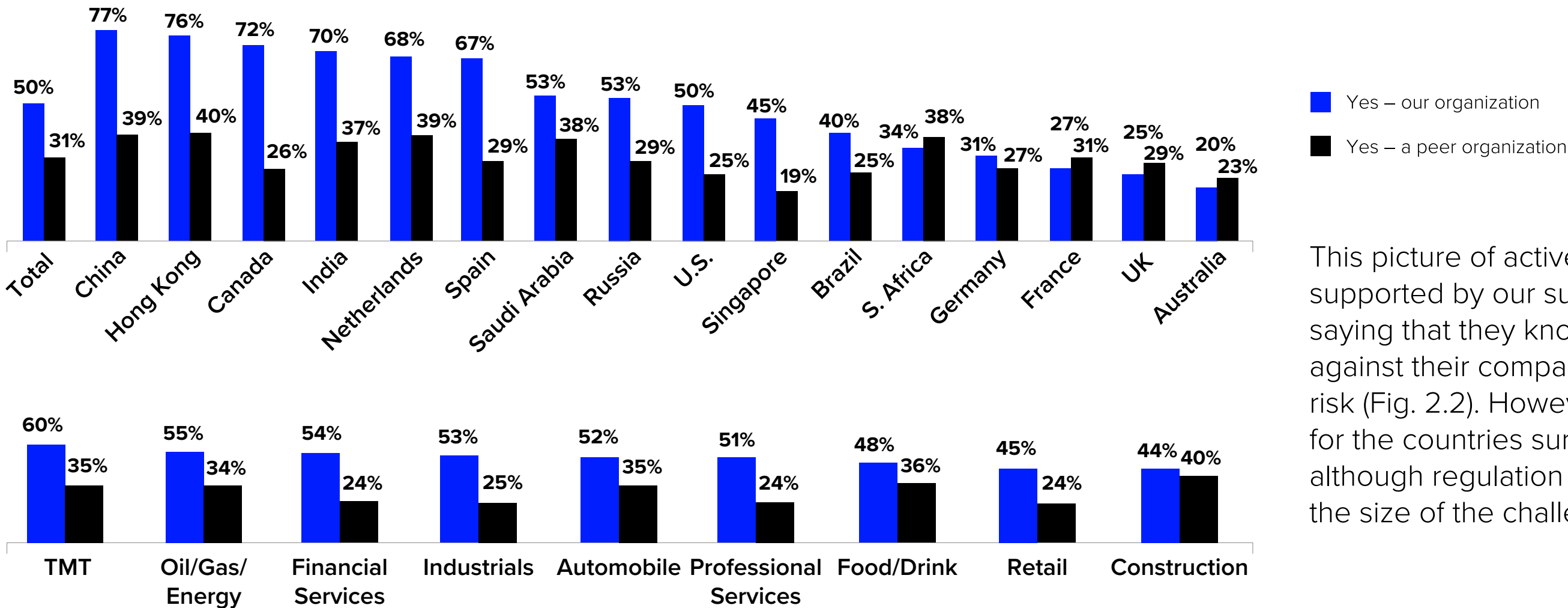




Figure 2.2: Enforcement action

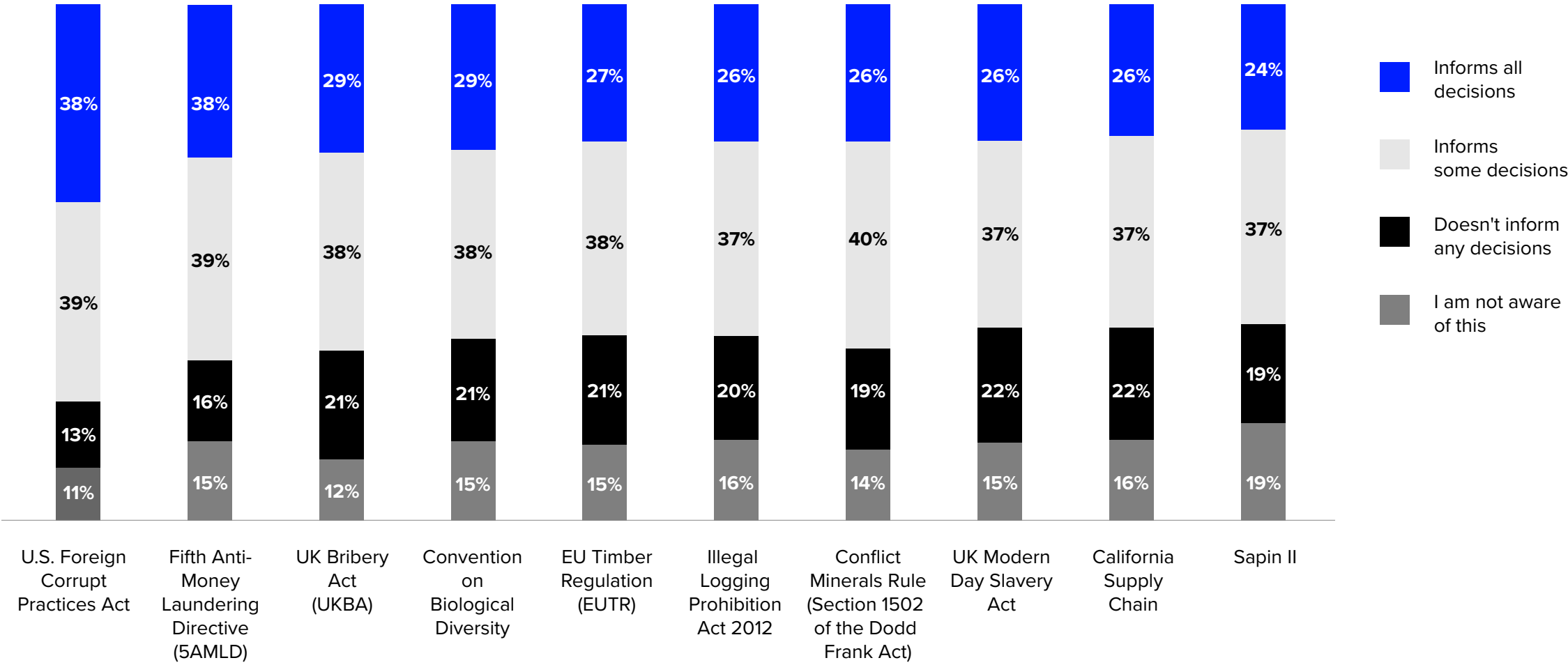
Has your organization or a peer organization had an enforcement action in relation to third-party risk that you're aware of? (Please select all that apply)



This picture of active and effective regulators is supported by our survey, with 50% of respondents saying that they know of an enforcement action against their company in relation to a third-party risk (Fig. 2.2). However, this has decreased by 2% for the countries surveyed in 2016, suggesting that although regulation has become tougher, so has the size of the challenge.

Figure 2.3: Total: Informing third-party risk management

Which of the following guidelines, legislations, frameworks and standards do you use to inform your decisions on third-party risk management? (Please select one column response for each row)



As illustrated in Fig. 2.3, while the vast majority say that they use global regulations like the U.S. Foreign Corrupt Practices Act (77%), the Fifth Anti-Money Laundering Directive (69%) and the UK Bribery Act (67%) to inform their decisions on third-party risk management, that still leaves significant minorities who do not.

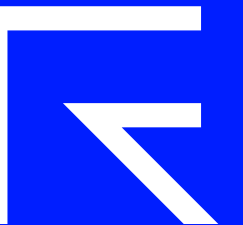


# IS YOUR INVESTMENT TAKING ACTION OR TALKING ACTION?

Transparent Environmental, Social and  
Governance data, covering 400+ metrics.  
Get a more detailed picture.

[refinitiv.com/ESG](https://refinitiv.com/ESG)

REFINITIV<sup>®</sup>  
DATA IS JUST  
THE BEGINNING<sup>®</sup>





Just over six in 10 (61%) of survey respondents believe that prosecution would be unlikely if they breached third-party related regulations. This is despite the perception that, if they did get caught in a regulator’s crosshairs, the impact could be catastrophic. When asked about the negative impact on corporate value if their organization or third parties breached regulations, the average estimate was 25% (Fig. 2.4). In other words, a quarter of their organization’s share price could be lost.

The impact was calculated to be even higher in the financial services sector (28%) and lowest in retail (21%). When we asked institutional investors globally about the extra corporate value they would attribute to a company with a high environmental, social, and governance (ESG) rating, the mean was 36%.

Figure 2.4: Negative impact of third-party regulatory breaches

If your organization or third parties breached regulations, what do you think the negative impact would be on corporate value? (Please select one response)

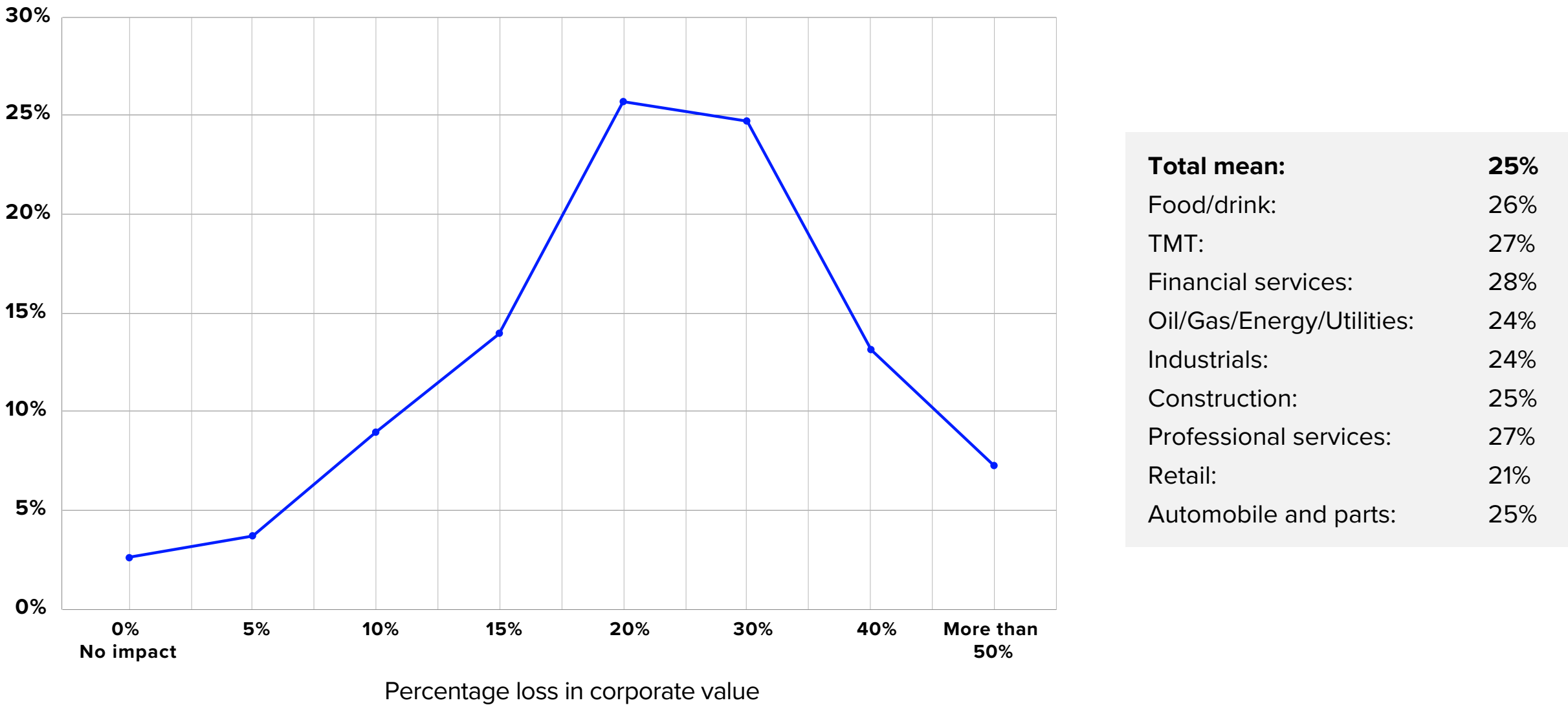
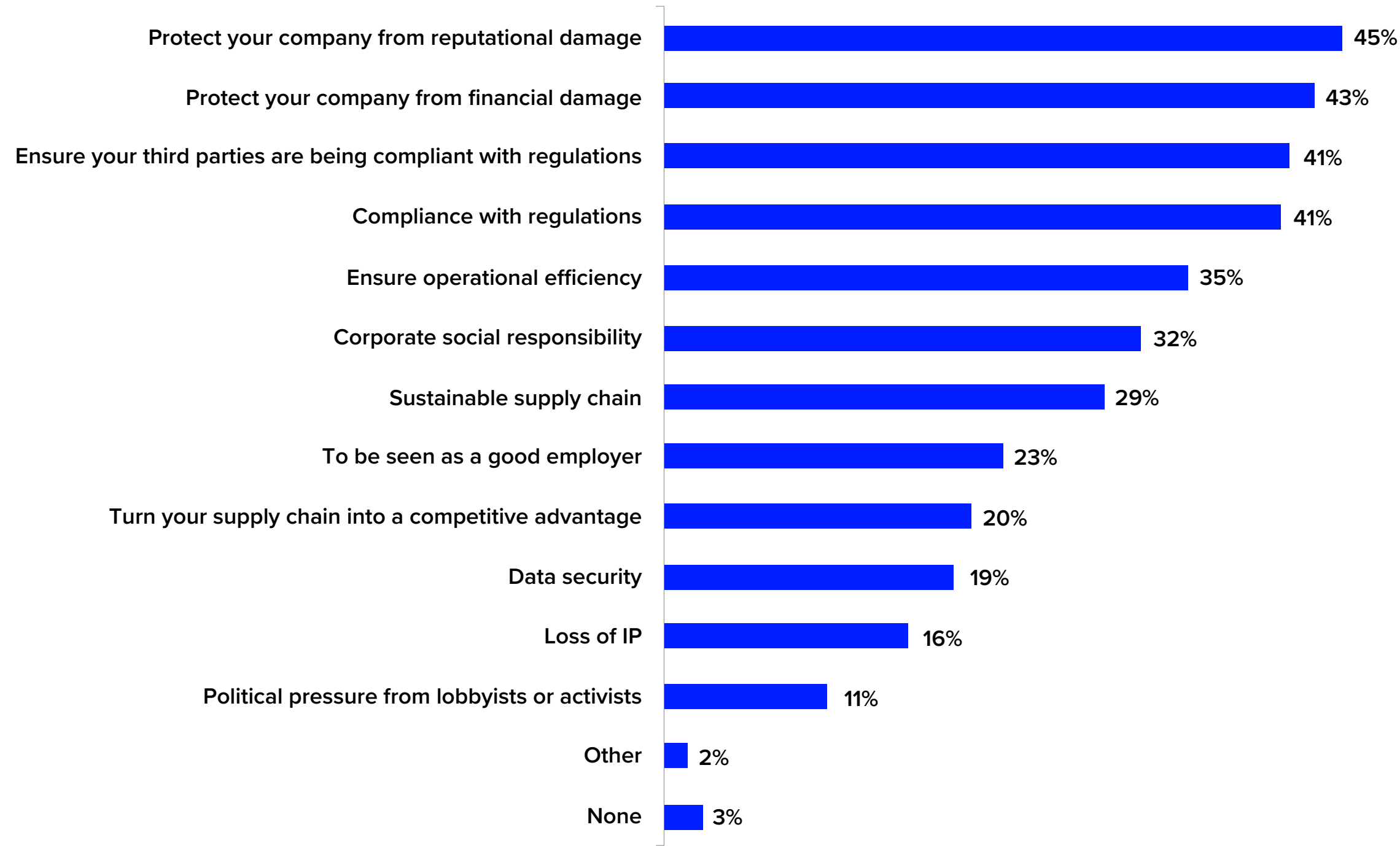




Figure 2.5: Total: Reasons to conduct due diligence on third parties

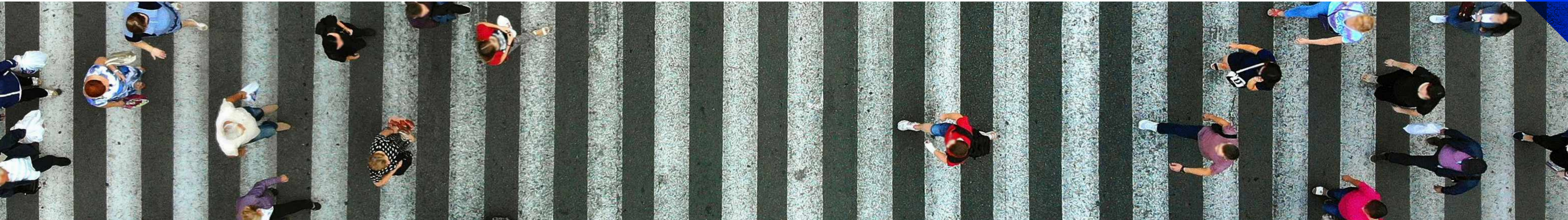
Which of the following do you consider are particularly important reasons the conduct due diligence on third parties? (Please select all that apply)



## Reputational and financial risks dominate

When asked to identify the most important reasons to carry out due diligence on third parties (Fig. 2.5), 45% said it was to protect themselves from reputational risk and 43% cited financial risk, both marginally ahead of ensuring regulatory compliance at 41%. These three reasons far outweighed the additional benefits to organizations from carrying out effective due diligence. Fewer respondents believed that due diligence on third parties could bring organizational benefits, such as being seen as a good employer (23%) or ensuring operational efficiency (35%).

Since the COVID-19 pandemic, the wider organizational benefits of good supply chain risk management have become even more apparent, particularly around improving resilience through diversifying suppliers.





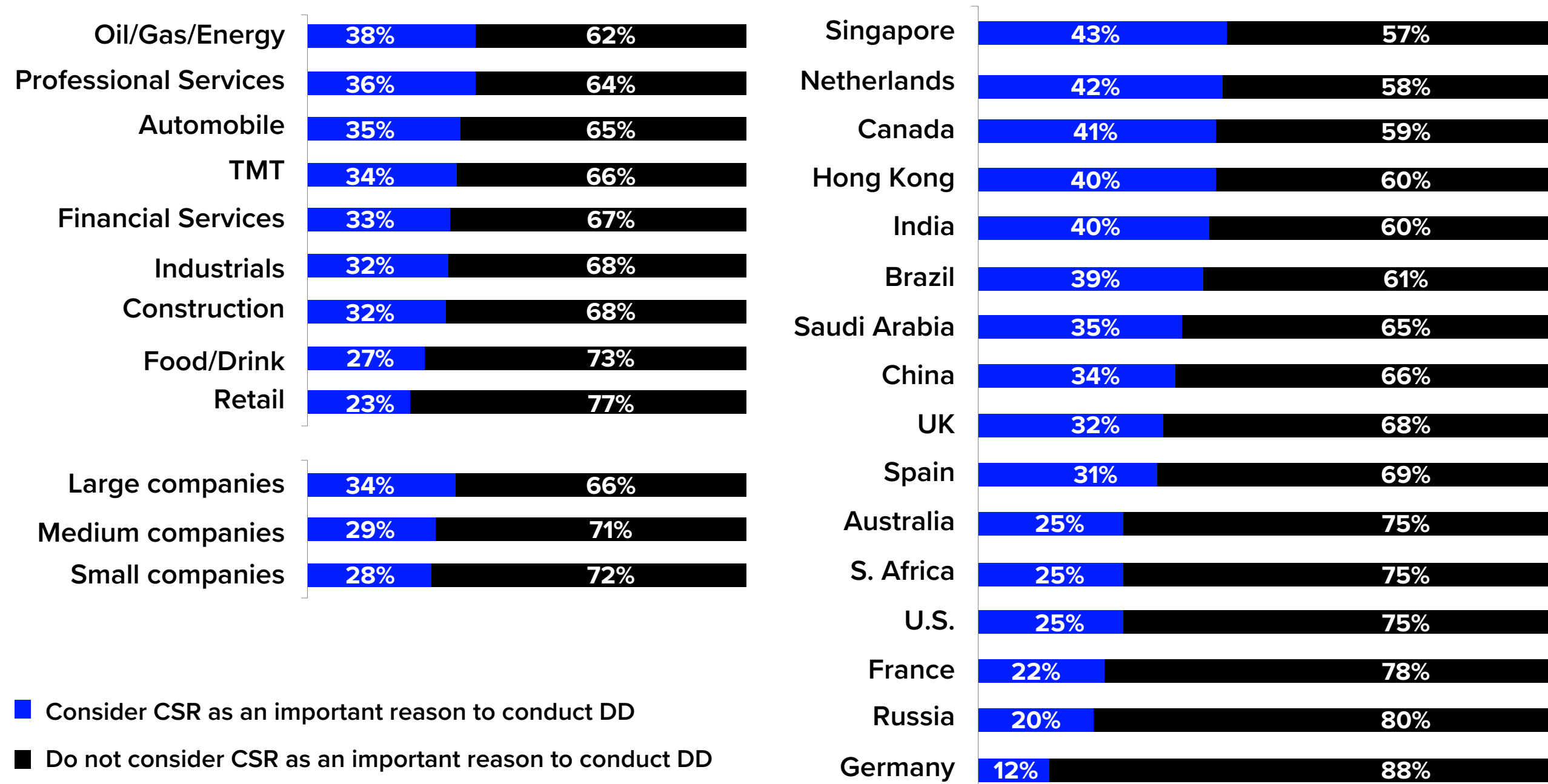
## Growing awareness of green risks – but more clarity is needed

Whether an organization wants to make sure it meets its own corporate social and governance (CSR) standards, avoids unwittingly supporting green crime or ensure that its ESG position satisfies the requirements of ethical investors, third-party relationships can play a key role.

Awareness of green regulations appears to be high (Fig. 2.6) with, for example, The Illegal Logging Prohibition Act (64%) and Conflict Minerals Rule (67%) being regularly used to inform decisions on third-party risk management. And as a driver for conducting due diligence, CSR (32%) and supply chain sustainability (29%) are identified as being important by nearly a third of respondents. The use of green regulations to inform decisions on third party risk management has increased compared to when we asked the same countries 4 years ago. Meanwhile, CSR and a sustainable supply chain were considered similarly important reasons to conduct due diligence on third parties when compared to 2016.

**Figure 2.6:** Those who consider CSR as an important reason to conduct DD

*Which of the following do you consider are particularly important reasons to conduct due diligence on third parties? (Corporate Social Responsibility)  
(Please select all that apply)*



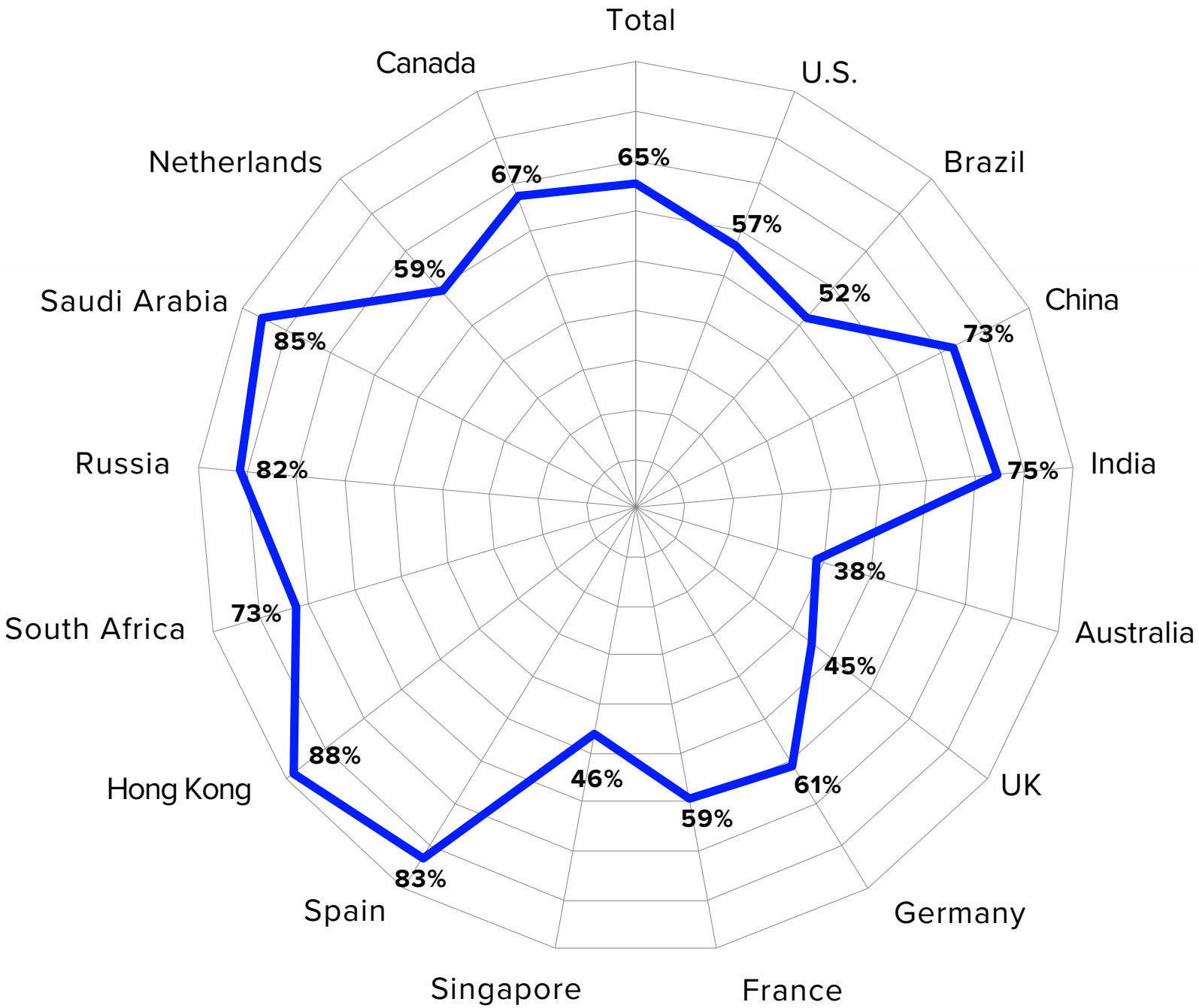
**Nearly six in 10  
(57%) suspect  
listed companies of  
'greenwashing' by  
providing misleading  
environmental  
credentials.**





Figure 2.7: Illegal activities

Do you know of suspect any of your third-party suppliers or their suppliers have been involved in any of the following?



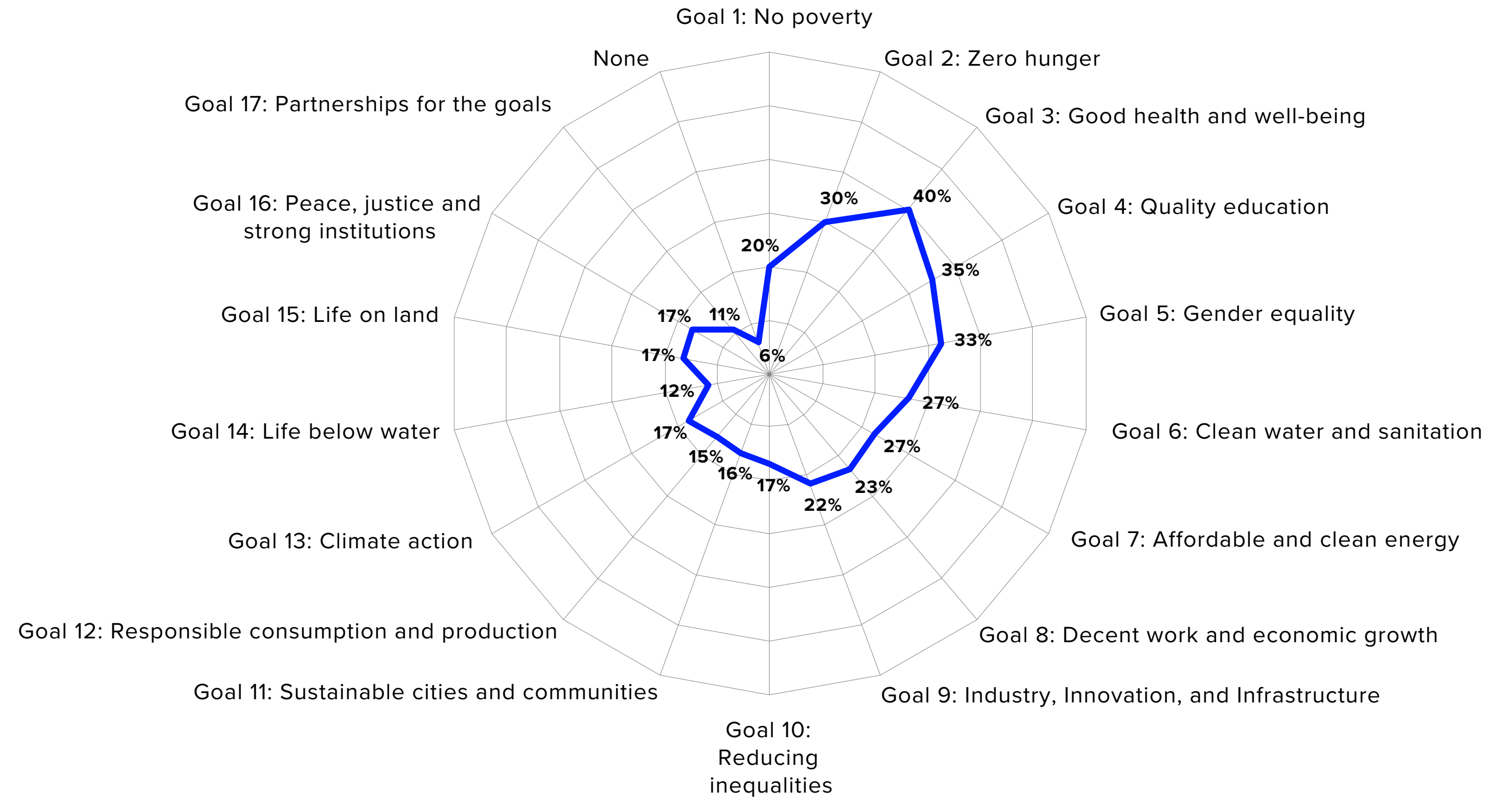
A substantial 65% of respondents know or suspect that third parties they conduct business with may have been involved in a range of illegal, environmentally damaging activities (Fig. 2.7).





**Figure 2.8: Sustainable Development Goals (SDG)**

*Which of the SDGs is your company actively trying to support? (Please select all that apply)*



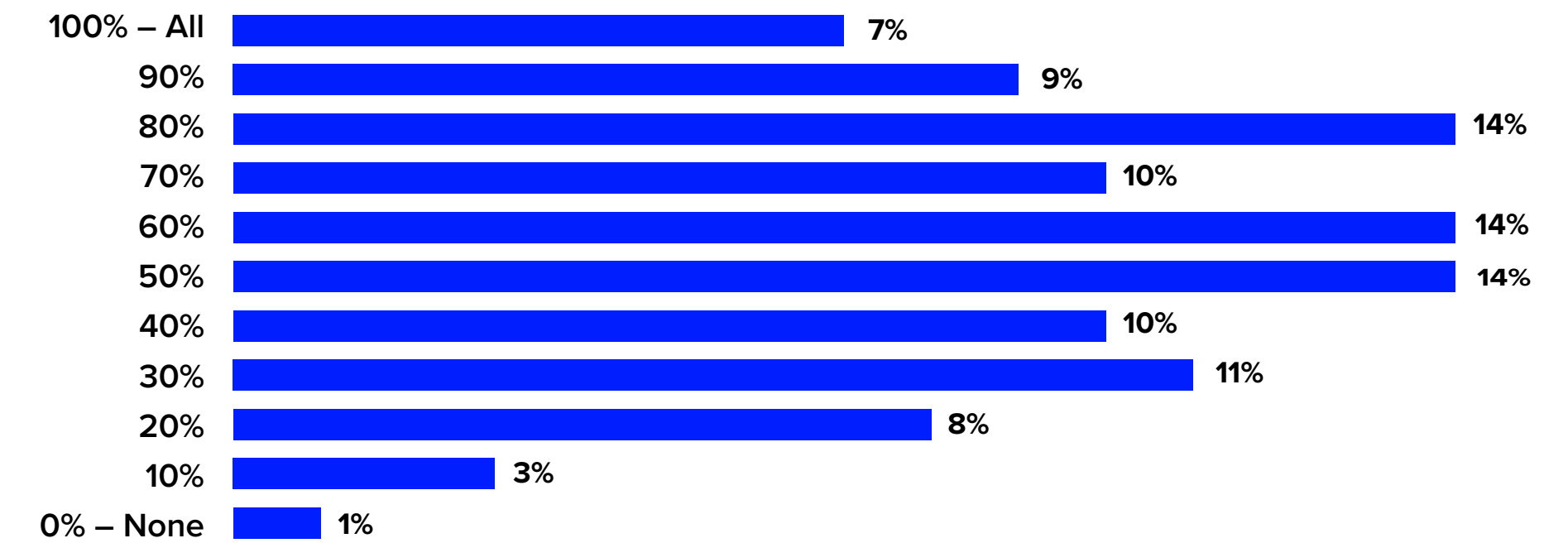
Yet, while almost 94% of respondents say that their organizations support at least one of the UN sustainable goals (Fig. 2.8), it's notable that climate action (17%) falls well behind health at 40%, education at 35% and gender equality at 33% in terms of priorities.



One reason for the mixed messages may be a lack of certainty over green credentials in the view of global institutional investors. Nearly six in 10 (57%) suspect listed companies of ‘greenwashing’ by providing misleading environmental credentials, and 84% think this is becoming increasingly common (Fig. 2.9). This demonstrates the need for independent and robust due diligence.

**Figure 2.9:** Suspicion of companies involved in ‘greenwashing’

*Approximately what percentage of listed companies would you accuse of ‘greenwashing’ (misleading company environmental credentials)?*

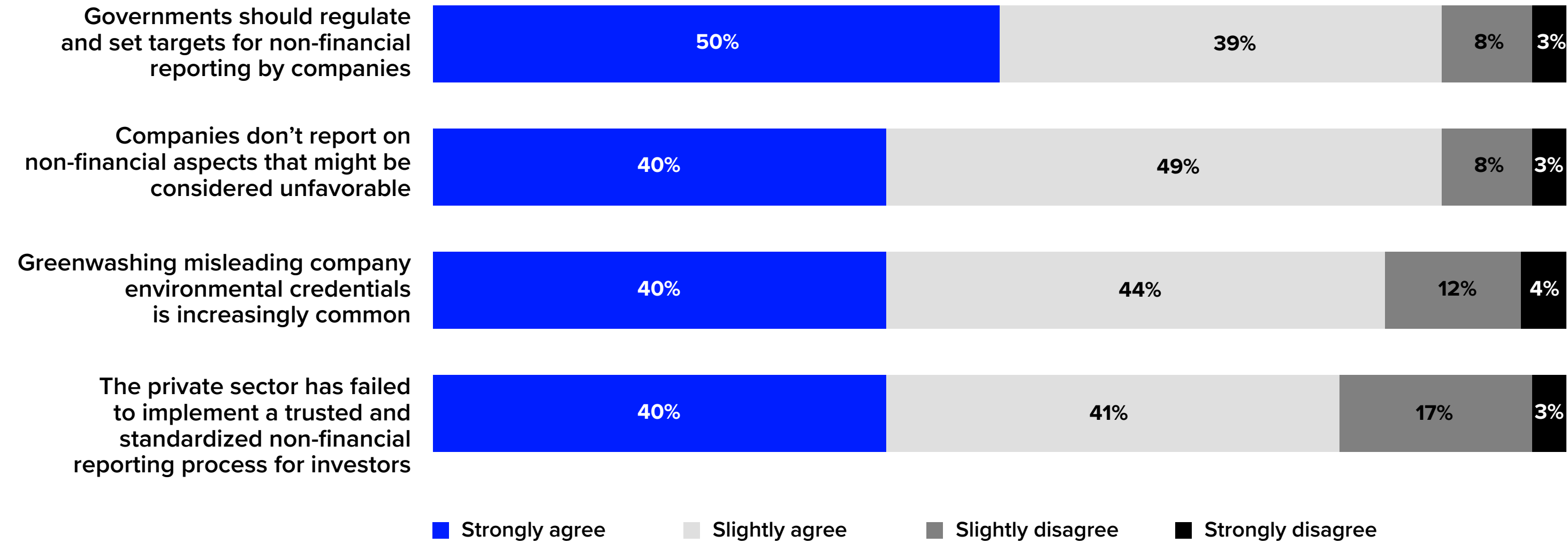


**Mean: 57%**



**Figure 2.10: Opinions on current non-financial reporting**

How strongly do you agree or disagree with the following statements with regards to the following? (Please select one column response for each row)



Respondents to our survey of institutional investors are clear that action needs to be taken in this area, with 90% saying that governments should regulate and set targets for non-financial reporting (Fig. 2.10). And 81% agree that the private sector has failed to implement a trusted and standardized non-financial reporting process for investors. If organizations lack clarity over how to evaluate the environmental risks associated with third parties, the danger is that they are less likely to measure and monitor them.



## 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.



## INTERVIEW

# GLOBAL POLICING CHALLENGES IN THE COVID-19 WORLD

Jürgen Stock, Secretary General, INTERPOL

COVID-19 is a social and public health crisis of a magnitude most of us have never seen, nor could have imagined. It is of no surprise that criminals have already taken advantage of the fear and vulnerability which this pandemic has brought.

Law enforcement agencies worldwide, like all public and private sector bodies, are facing unprecedented challenges and pressures; in particular, new ways of policing in response to a significantly altered working environment and responding to evolving types of COVID-19-linked criminal activity.

In recent months, we have seen a significant increase in criminal activities in cyberspace, particularly fraud schemes relating to personal protective equipment, vaccines, self-testing kits, protective sprays and other health products.

When life-saving products or a vaccine are available, demand will soar resulting in a parallel increase in theft and counterfeiting of these important medicines. We will all need to be ready. INTERPOL is already looking at how we can assist countries to effectively track legitimate stocks of medical goods, or prevent their diversion. Similarly, the likelihood of organized crime groups infiltrating the legitimate economy should not be underestimated.

The danger already existed before the confinements began, as mafia organizations have long invested in essential activities such as the agro-food sector, the supply of medicines and medical equipment, road transport, funeral services, cleaning services and waste disposal.

The amount of cash capital they have means these organizations are well placed to offer assistance such as guaranteeing payments, or offering loans to struggling companies.

Ensuring that post-emergency stimulus packages remain within legitimate circuits and do not end up increasing the financial power of mafia-type organizations is also crucial and will require close oversight.

When this pandemic ends, although we will be operating in a radically changed environment, the importance of public/private sector cooperation will not have changed. The unique global role of INTERPOL will not have changed.

INTERPOL remains committed to our vision of connecting police for a safer world, especially as COVID-19 has made it clear that more than ever, everyone's security relies on global collaboration.

---

**“Everyone’s security  
relies on global  
collaboration.”**



## INTERVIEW

# AN INTEGRATED, ETHICAL APPROACH TO THIRD-PARTY RISK

Alison Taylor, Executive Director, Ethical Systems

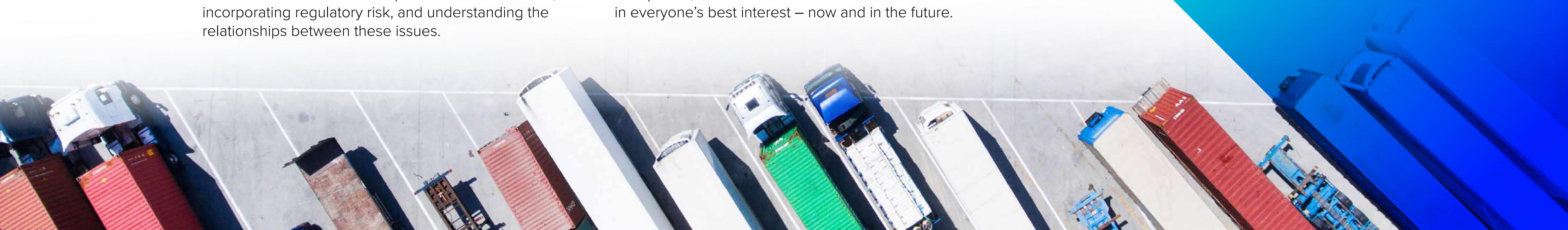
While third-party due diligence practices are core elements of the Foreign Corrupt Practices Act 1977 (FCPA) and other prominent anti-bribery standards, they tend to focus on distributors, sales agents and advisers. Supply chain risk is often managed by distinctly separate teams and processes and is usually based on self-reported information backed by limited, on-site audits that focus on environmental and social performance.

This two-track process has become untenable. Public scrutiny of supply chain practices has increased, regulation of modern slavery and trafficking has advanced, and the connections between corporate responsibility and regulatory compliance have grown far clearer. Drawing a firm distinction between regulatory requirements on one hand and environmental and social performance on the other isn't practical; after all, a supplier that treats employees poorly or violates environmental standards is more likely to disregard anti-bribery provisions as well. This makes a strong case for a due diligence process that considers environmental, social, and governance issues in a more holistic manner, bringing more rigor to disclosure on environmental and social performance evaluation, incorporating regulatory risk, and understanding the relationships between these issues.

It is understandable that, as this survey shows, companies seem overwhelmed by the scale of the oversight challenge, particularly given their need to look deeply into the entire supply chain, not just the first tier. They are hard-pressed to manage cost and volume. Growing transparency is a cause for optimism, but companies today are struggling over a lack of consensus on what good supply chain oversight looks like – and how far they need to go to meet expectations. Suppliers are themselves calling for additional support and assistance from large customers regarding integrity challenges, particularly in countries with endemic corruption, but the large multinationals with the capacity and negotiating power to help them worry about regulatory exposure.

What will change require? We need to commit to a more realistic conversation that includes investors, regulators, companies, and civil society, and we need to build a model that includes the rigorous data analysis afforded by the best third-party oversight tools and also the engagement and capacity-building of the best supply chain-engagement practices. This would help us build more effective, transparent, collaborative value chains. This is what lies in everyone's best interest – now and in the future.

**“This two-track process has become untenable.”**





## INTERVIEW

# RAISING OUR RESPONSE TO WILDLIFE CRIME

John Cusack, Financial Crime Fighter, focused on Green Crimes including wildlife crime and human trafficking

In my role as an Ambassador to the Royal Foundation's United for Wildlife Financial Taskforce, I see first-hand how many people in the corporate world, both in financial institutions as well as businesses involved in, for example transport and logistics, are committed to raising their response to combatting wildlife crime. Many of these are also involved in combating other areas of green crimes as our 'environment' is targeted by criminal enterprises for financial gain. This genre of crimes is not abstract and accounts for significant and growing levels of criminal activity at the same time as robbing countries who are least able to respond to biodiversity loss and protect local essential resources, on an industrial scale.

That's why I was disappointed to see the results from Refinitiv's report, which reveals that just 26% of respondents are knowledgeable about environmental

crime and its associated risks, whilst at the same time 65% of respondents know or suspect that third parties they could be dealing with may have been involved in illegal or environmentally damaging activities. These numbers reflect the reality that more needs to be done, and quickly. There are a number of ways that awareness and knowledge of the threats from green crimes can be improved, as well as strengthening due diligence on third-party relationships.

This is why I welcome Refinitiv's work to shine a brighter light on this increasingly important issue and their ability to support corporates that want to better protect themselves – and in so doing reduce the scope for criminals to do business with legitimate enterprises.

**“These numbers reflect the reality that more needs to be done, and quickly.”**





## INTERVIEW

# GREATER ENFORCEMENT ACTION IS REQUIRED

Tom Keatinge, Director of RUSI's Centre for Financial Crime and Security Studies

This new Refinitiv third-party risk survey makes depressing reading. Every year, the business operating environment becomes more heavily regulated; the responsibilities placed on business proliferate yet the issues that these regulations seek to combat persist. And they persist because the implementation of these regulations is lacking; not entirely, but given the extent to which the range of global threats considered in this survey continue unchecked, the contribution made by industry can clearly go further.

Despite the importance placed by institutional investors on adherence to ESG standards, this survey reveals that nearly two-thirds of respondents do not believe they would be prosecuted if they breach third-party related regulations.

A further striking finding is that the most important reason to carry out due diligence on third parties is revealed to be company-centric: protecting from reputational and financial risks, well ahead of addressing wider societal and environmental issues.

Finally, perhaps most shocking is the revelation that institutional investors believe that nearly 60% of listed companies are 'greenwashing' by providing misleading

environmental credentials, and 84% think this is becoming increasingly common.

So, what should we take away from this valuable survey? In short, there is much to do if businesses are to be the forces for good – not just profit – that many claim to be. It also shows us the importance of states and their industry supervisors and regulators auditing the implementation of regulations and taking meaningful enforcement action against those companies that fall short. The past penalties issued against banks for compliance failings and against chemical or extractive companies for environmental damage have driven major upgrades in standards. Likewise, those within the industry that genuinely care must drive change. If industry groups develop third-party required standards that exclude those that fall short from their combined supply chain, standards will inevitably rise.

If the COVID-19 pandemic crisis teaches us just one thing, it is the importance of maintaining values in the way we engage with society and the environment. This latest third-party risk survey suggests there is plenty more work to be done.

---

**“The issues that these regulations seek to combat persist.”**



# Enhanced due diligence

Enhance. Simplify. Protect.

Advanced background and integrity checks on any entity or individual, anywhere in the world. Protect your reputation, meet regulatory obligations and understand exactly who you are doing business with.

[refinitiv.com/edd](https://refinitiv.com/edd)

**REFINITIV**<sup>®</sup>  
DATA IS JUST  
THE BEGINNING<sup>®</sup>





# 3 | TAKING ACTION

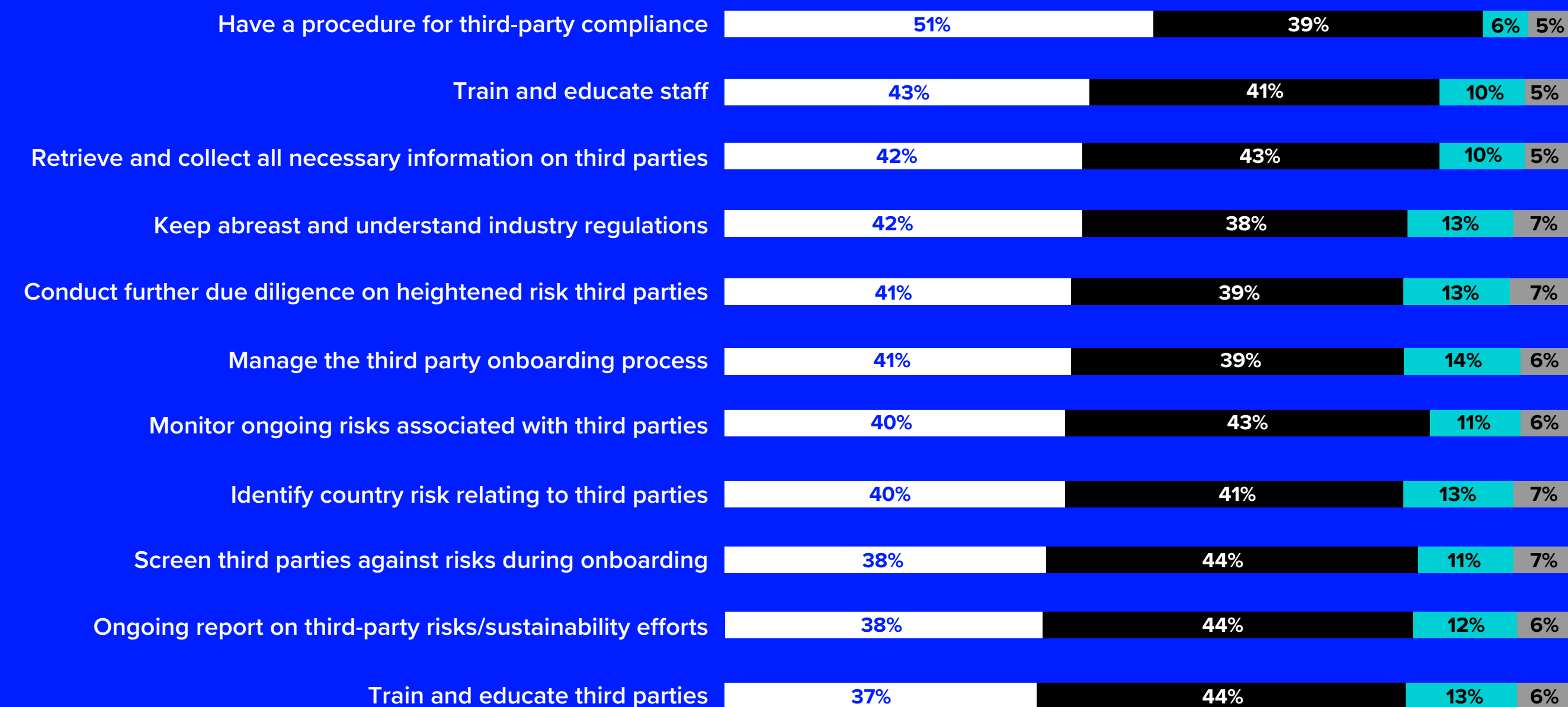
## INNOVATION AND COLLABORATION CAN HELP ORGANIZATIONS RISE TO THE CHALLENGE

### Current procedures

When asked what actions their company currently takes to manage third-party risk (Fig. 3.1), only around half (51%) say that they have procedures fully in place for third-party compliance, leaving 45% with procedures only partly in place or not at all. The next most likely action is training and education for staff, with 43% having fully implemented this and 51% only doing so partly or not at all. Clearly, this leaves room for improvement.

**Figure 3.1:** Managing risk with third parties

*What steps does your company currently take in regards to managing risk with third parties in your supply chain? (Please select one column response for each row)*



Only 42% say that they keep fully abreast of regulatory information, which is a cause for concern given that 68% think that the amount of regulatory information published by regulators over the next 12 months will increase. Just over two-thirds (67%) say that although they know where risks may materialize, they struggle to employ the processes necessary to detect them.

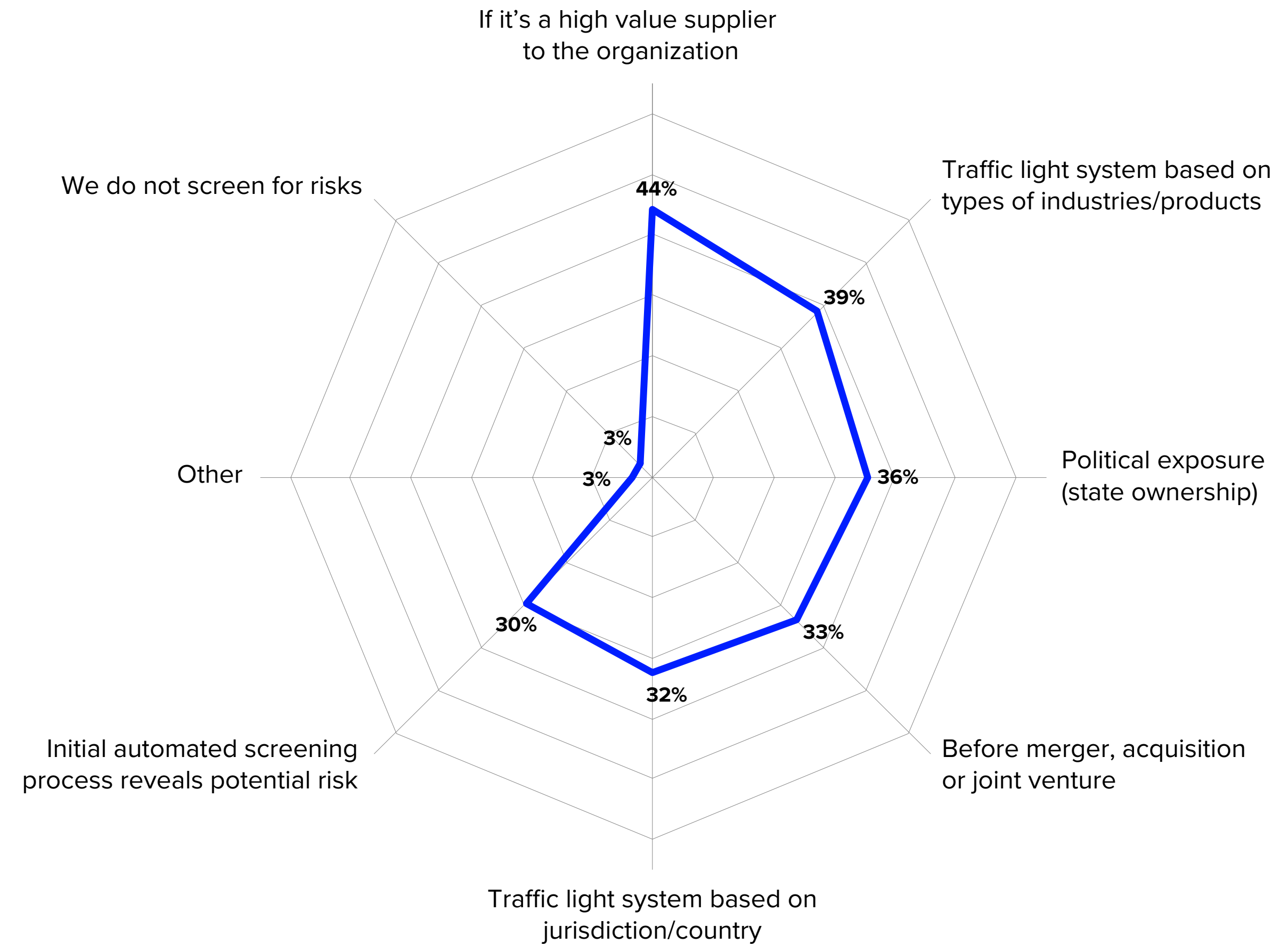


## Drivers for due diligence

The most common lever for carrying out further due diligence (as shown in Fig. 3.2), is the high value of the supplier to the organization (44%) and a traffic light system based on industry/sector (39%). More holistic factors such as political exposure (36%) and jurisdiction/country risk (32%) rank lower, with the retail sector (18%) well below average for the latter. In the professional services industry, 6% say that they do not screen for risks at all, twice the overall average of 3%. This suggests that organizations need to deepen and broaden their approach to due diligence.

**Figure 3.2:** Determining further due diligence

*How do you determine if further due diligence needs to be conducted on a third-party? (Please select all that apply)*





## Screening activity and knowledge of risks

When it comes to what level of the third-party ownership structure is screened, 45% screen the parent company, but only 35% investigate Ultimate Beneficial Owner (UBO) and just 32% delve into subsidiary level (Fig. 3.3).

Figure 3.3: Level of third-party ownership structure currently screened

*What level of third-party ownership structure would you typically screen? (Please select all that apply)*

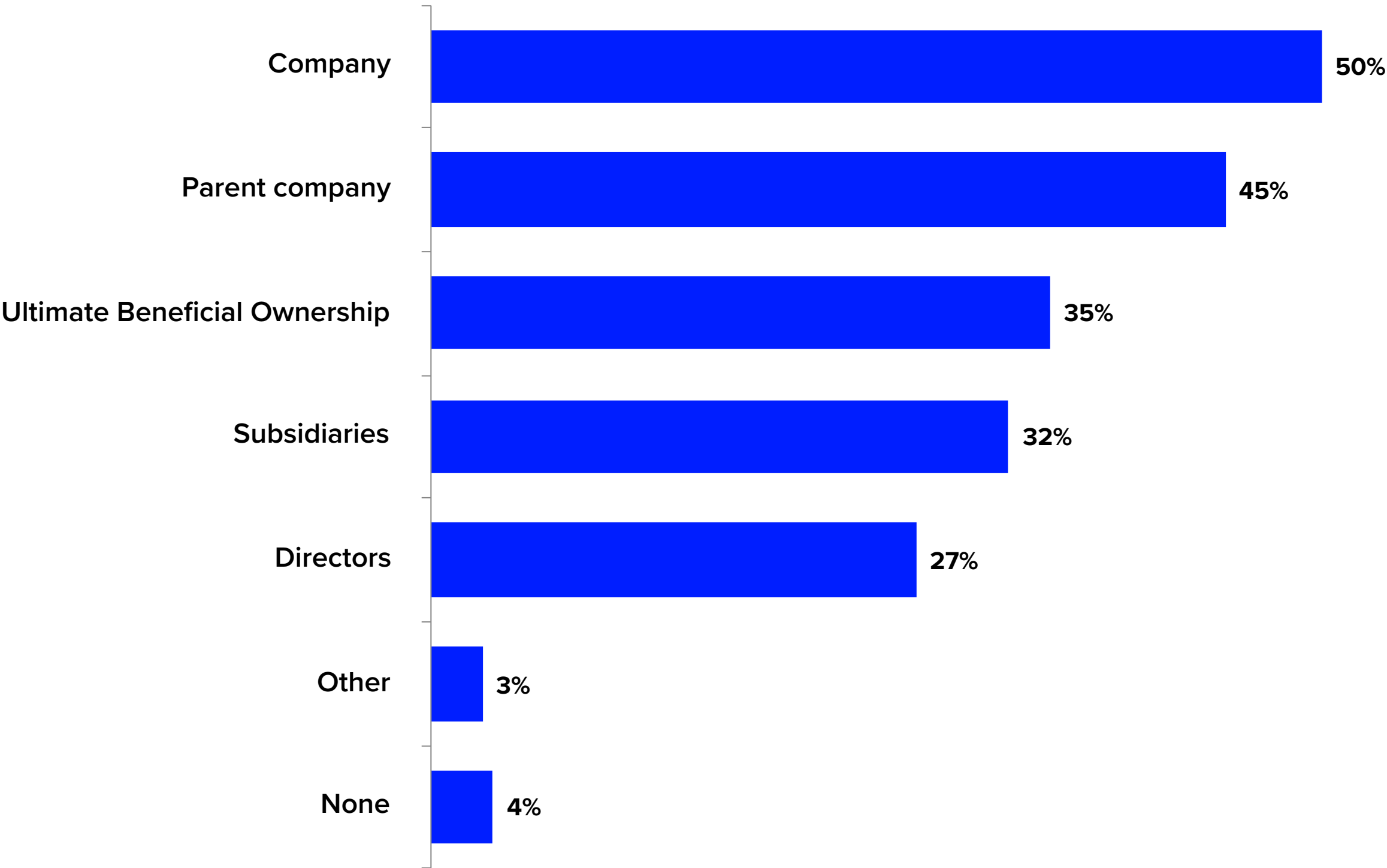
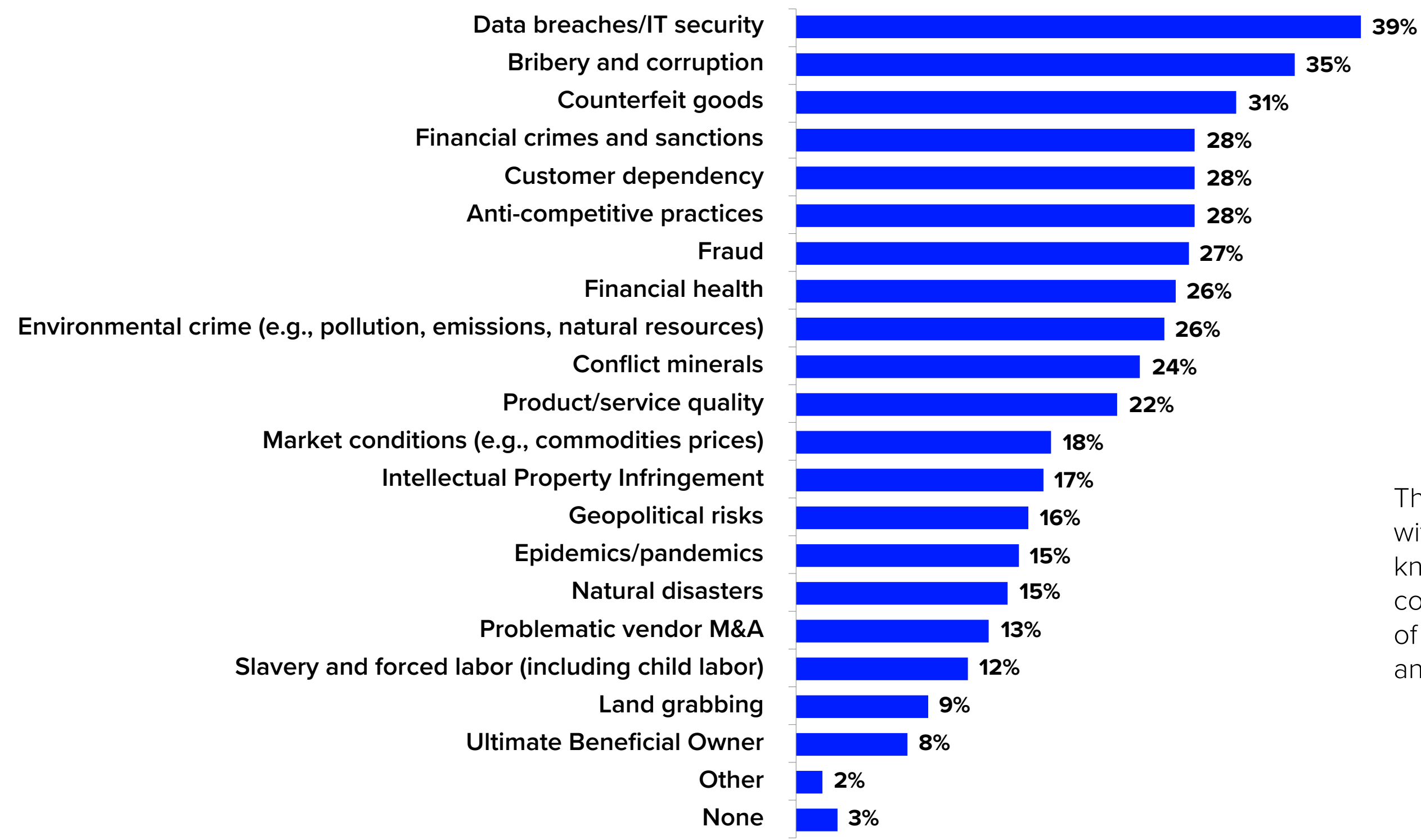




Figure 3.4: Knowledge levels of various risks

Which of the following risks are you sufficiently knowledgeable about? (Please select all that apply)



These gaps in screening are mirrored by knowledge gaps, with less than four in 10 claiming that they have sufficient knowledge on any of the major elements of risk for their company (Fig. 3.4). The risks that they have most knowledge of are data breaches and IT security (39%) followed by bribery and corruption (35%).

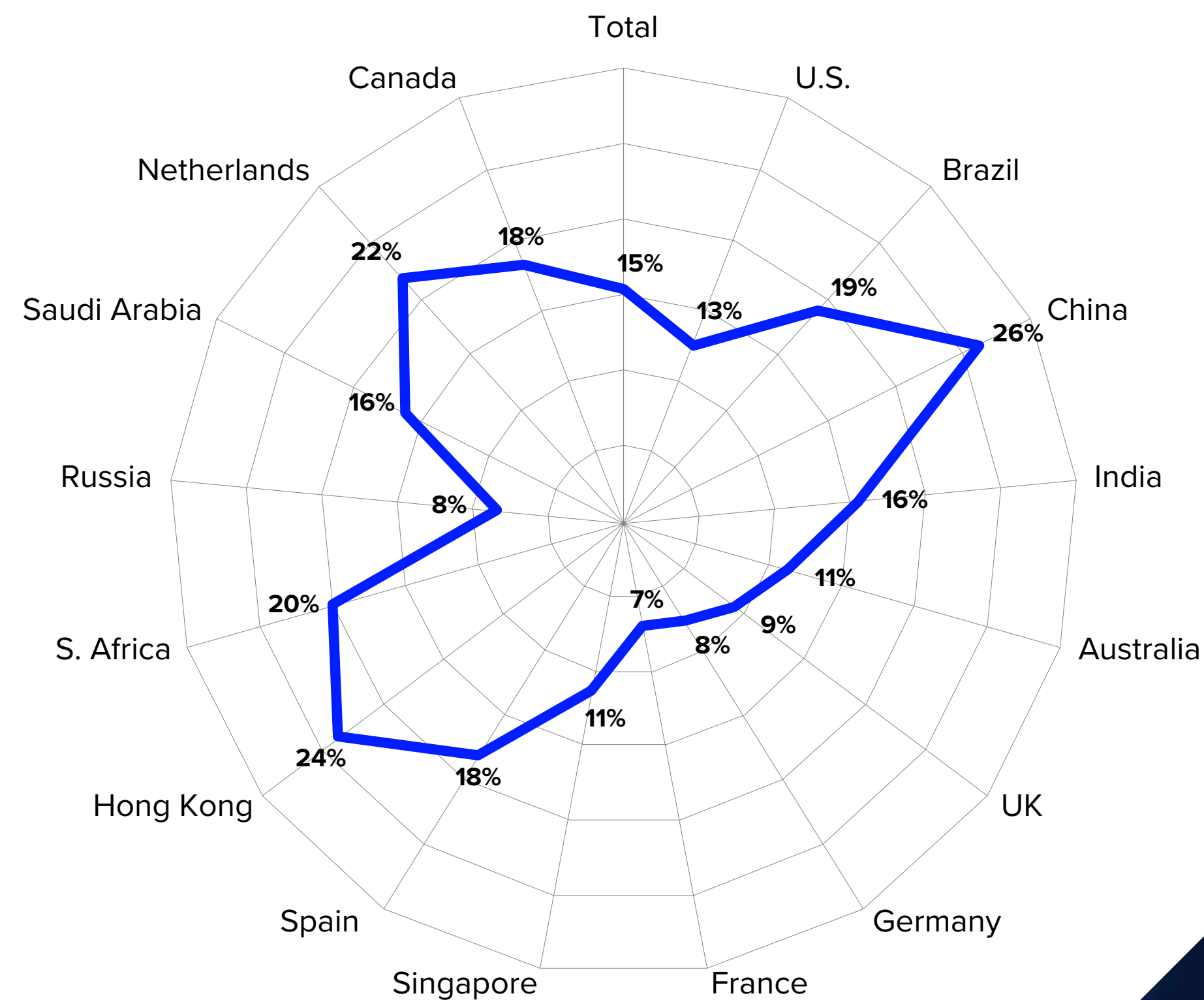


## Pandemic risks

In light of COVID-19, it is notable that respondents in China scored their knowledge of risks related to epidemics and pandemics above that of any other region (Fig. 3.5). This may reflect the fact that, at the time the survey was conducted, the majority of reported COVID-19 cases were in China. However, levels of awareness were universally low, with just over a quarter (26%) of China respondents confident that they had sufficient knowledge of the risks associated with pandemic and epidemics, compared to only 15% globally.

**Figure 3.5:** Knowledge levels of epidemics/pandemics, divided by country

*Do you feel that you are sufficiently knowledgeable about levels of epidemics/pandemics?*



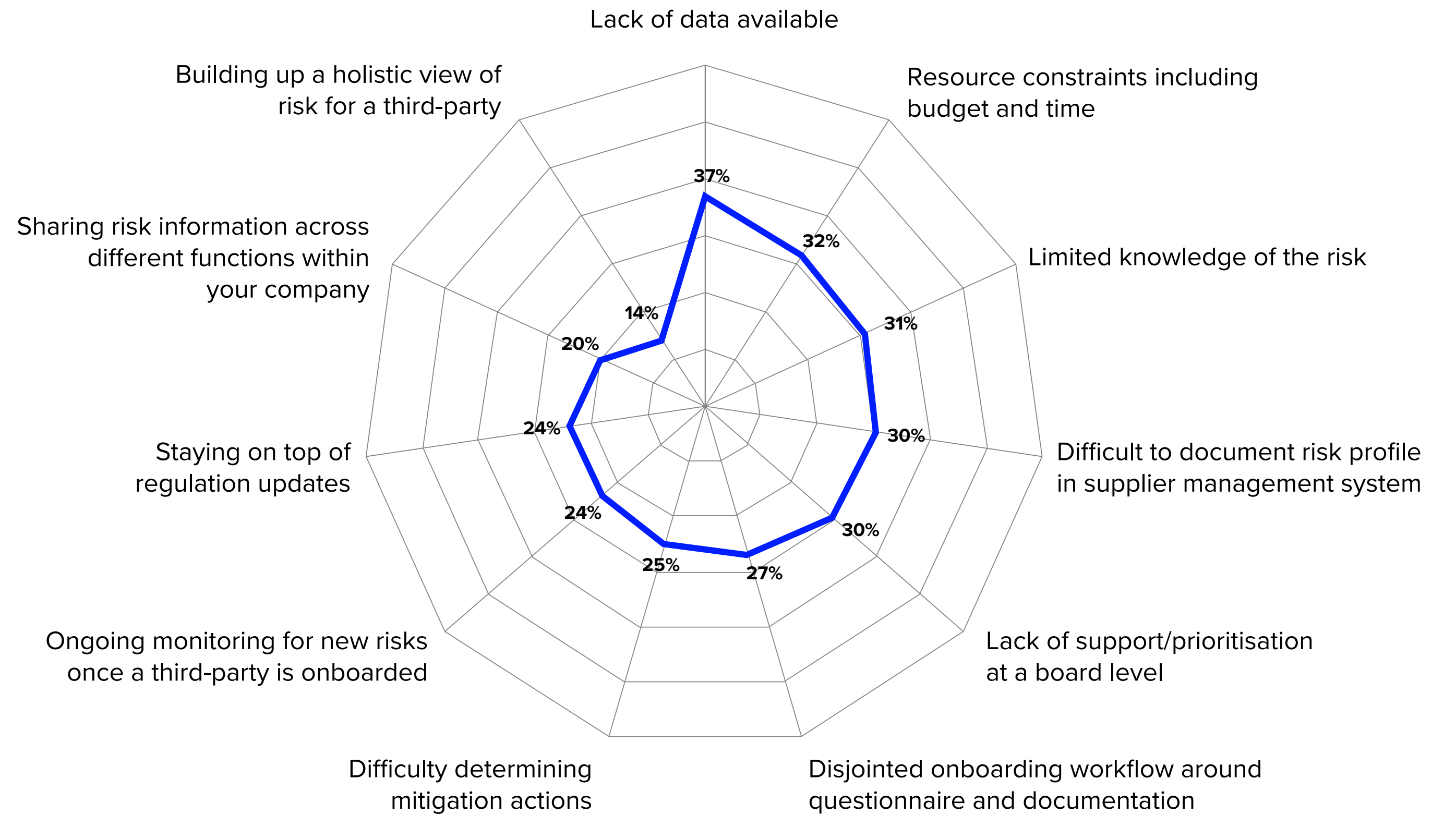


## The resources needed to reduce risk

Given the sheer volume of third parties that our respondents engage with, it's perhaps not surprising that resources are a key issue. Nearly a third (32%) cited a lack of time and money as constraining their ability to identify risks (Fig. 3.6).

**Figure 3.6:** Main challenges of implementing the right approach to identifying risk

*What challenges does your company currently face in implementing the right approach to indentifying risk within your supply chain? (Please select all that apply)*

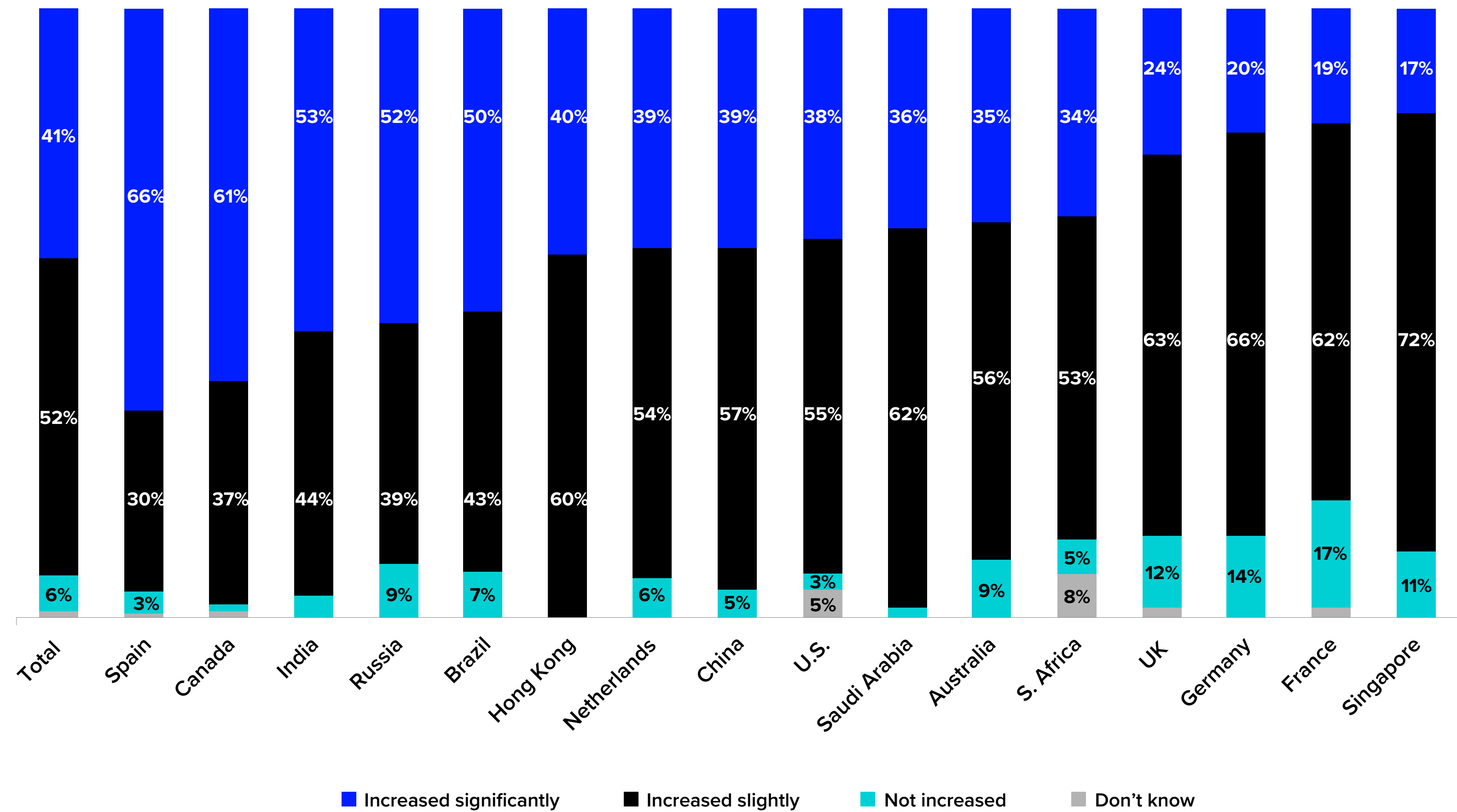




However, the cash is clearly available after the event, with a much larger 93% saying that spending increased after an enforcement action related to third-party risk (Fig. 3.7).

**Figure 3.7:** Changes to spending on compliance

*How has this changed the amount your organization spends on compliance? (Please select one response)*



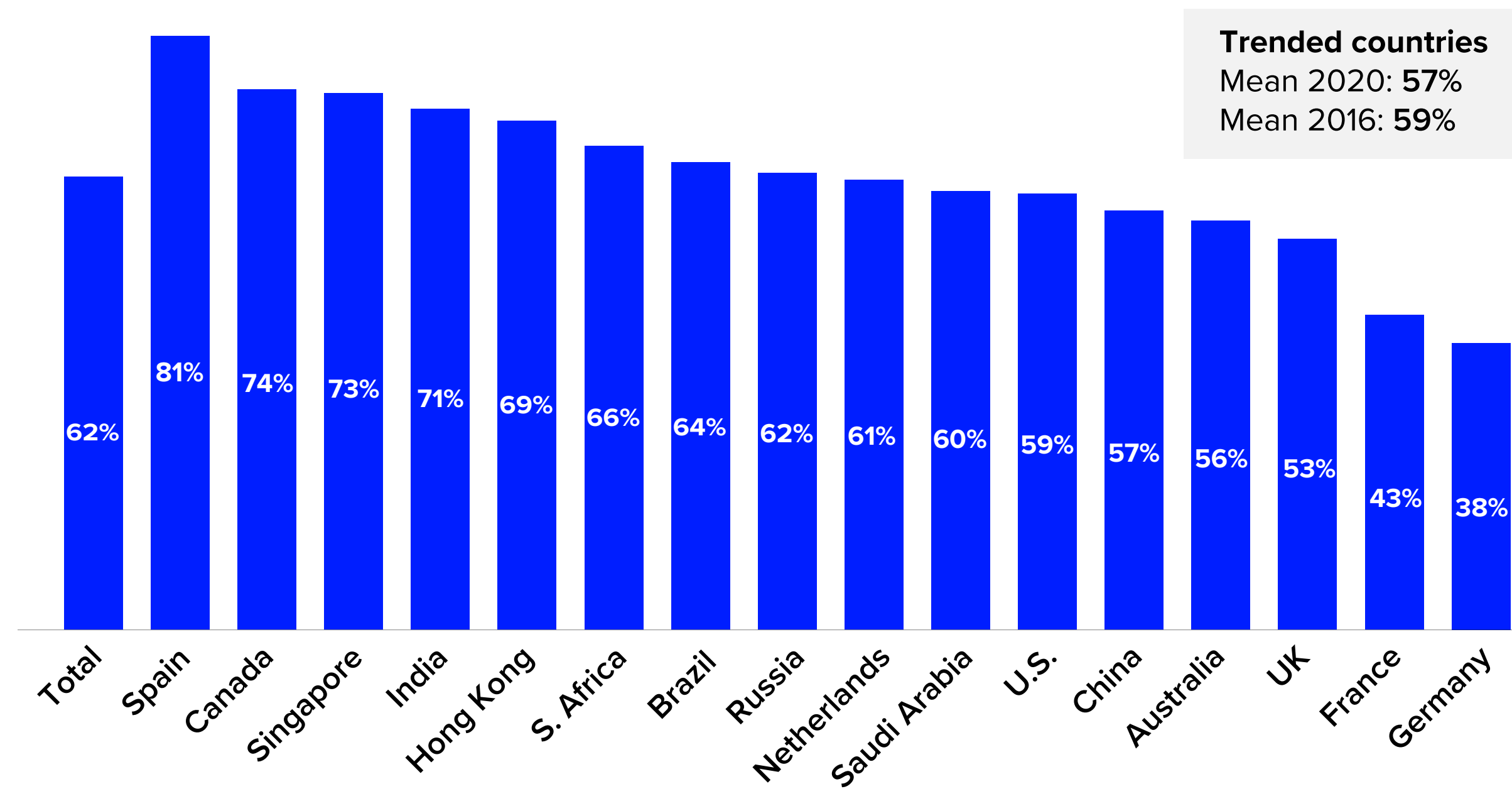


## Supply chains, COVID-19 and the data challenge

Complex global supply chains can create competitive advantages for businesses and cut costs for consumers, but they also carry risks. The key to managing these is having clear sight of, and doing due diligence on, all levels of the supply chain. Yet, our survey reveals that 62% of respondents do not know the extent to which third parties are outsourcing work (Fig. 3.8). For the countries surveyed in 2016, this has decreased from 59% to 57%.

**Figure 3.8:** Knowledge of the extent to which third parties outsource work

*How strongly do you agree or disagree with the following statement? "We do not know the extent third parties are outsourcing our work."*






COVID-19 has further exposed the fragility of supply chains and the important role that due diligence can play in identifying and managing the risks that threaten their stability. These include country risk and jurisdiction risk, as well as the concentration risk of overexposure to vendors or geographies.

COVID-19 is likely to be a key driver for organizations to build greater visibility and resilience into their supply chains. This new focus will encourage organizations to more thoroughly assess and mitigate supply chain risks and increase actions taken in all aspects of third-party due diligence.

Yet, in doing so, they must overcome the data challenge. In our survey, respondents say the biggest problem they face in identifying risk within their supply chain is lack of data (37%). This is significant because good quality data is crucial to unlocking the potential of the emerging technologies that can speed up compliance processes and better identify risks.



**“Lack of data  
is the biggest  
obstacle to  
identifying third-  
party risk within  
supply chains.”**



# RISING TO THE CHALLENGE

Refinitiv offers a full third-party risk solution that enables our customers to have an effective mitigation program from the initial screening and due diligence stages through to onboarding of their third parties. Our evolved approach to helping organizations to mitigate legal and regulatory risks uses a wide variety of trusted assets and leverages our breadth and expertise to assist with the identification of risks when conducting business with third parties across many use cases or operations, including:

- **Screening:** Check our market-leading World-Check Risk Intelligence database consisting of millions of records on individuals, entities and vessels to help identify potential risks in business relationships and networks.
- **Screening as a managed service:** We offer a managed screening service to carry out the screening and remediation on an organization's behalf. This allows our customers to reduce the overall costs of operations and resources dedicated to third-party risk management.
- **Country risk:** Determine any geopolitical, social and economic risks associated to the country in which the third parties are based.
- **Enhanced Due Diligence:** Detailed background reports on any third-party can assist in protecting against regulatory and reputational damage. Request specialized ESG reports.
- **Qual-ID:** Leveraging the World-Check Risk Intelligence data, Qual-ID helps uncover financial crime-related risk alongside a powerful identity network. Organizations can verify identification from trusted sources, proof legal documents, and screen for regulatory and financial risk – all in one transaction, via one API.
- **API to partners:** We have partnered with market-leading third-party software providers whose solutions can be integrated with our suite of products and services.





# CONCLUSION

Our interconnected business world not only increases the risks that an organization is exposed to through their third parties but also presents greater challenges in identifying and managing those risks.

That may explain why, despite stronger regulation and more powerful enforcement actions, organizations are less likely to carry out due diligence on third parties now than they were in our 2016 survey.

Failings in due diligence – whether at onboarding or ongoing monitoring – were made clear by the sudden escalation of COVID-19, exposing the cross-border vulnerability of supply chains and the limitations of business continuity plans.

The good news is that action is already being taken. More resources and greater technological innovation are helping organizations to get a clearer picture of risk. But more needs to be done. Although respondents cite a lack of data as the biggest challenge in identifying supply chain risk, the sheer volume of data when managing third-party risk can overwhelm organizations if not handled correctly.

The right tools are needed to structure and streamline that data in order to find the signal in the noise and pinpoint areas of higher risk. Here, it is clear that at Refinitiv we have a key role to play in helping organizations to rise to this challenge and unlock the full potential of innovation.

Our ESG data covers nearly 70% of global market cap and over 400 metrics, putting us in a strong position to help organizations address challenges, highlighted in our survey, to monitoring third parties' environmental performance. But this also requires collaboration. Refinitiv has joined The Future of Sustainable Data Alliance (FoSDA), which is working in partnership with the World Economic Forum to use data to drive the acceleration of sustainable finance.

Yet, as contributors from INTERPOL, RUSI, Ethical Systems and United For Wildlife make clear, the challenges that individual organizations face are often part of a broader problem – one that requires both consensus and concerted effort to address. We look forward to working with clients, regulators and industries across the world to close the gaps that are exposed by this report.

**Join the conversation #FightFinancialCrime**



READ MORE FROM OUR  
RISK MANAGEMENT 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 humans victims exploited by criminal gangs which launder their gains through the financial system.

[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](#)

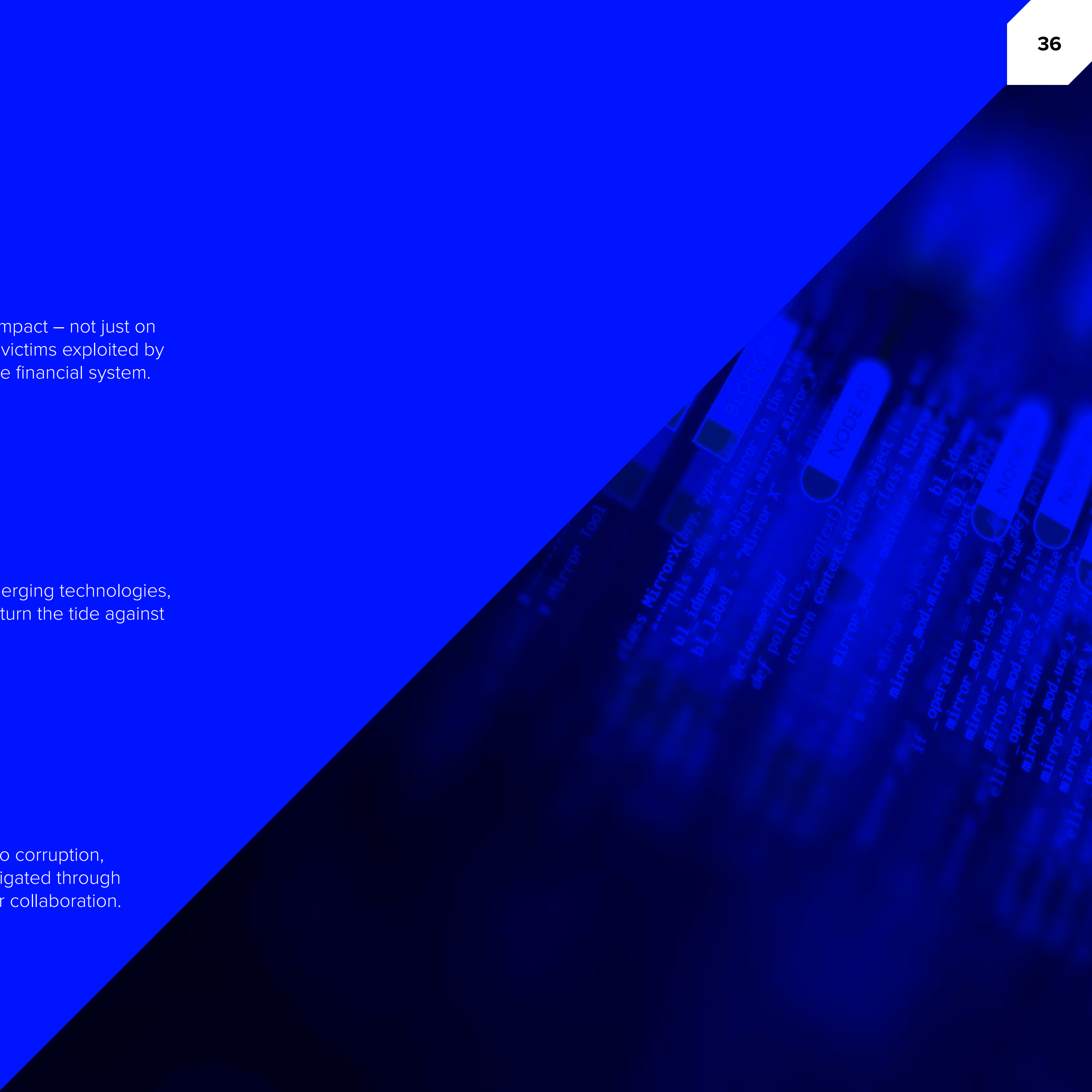


White Paper

Global sustainable development

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

[Read more](#)





Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community – driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

Visit **refinitiv.com**



RE1142653/6-20

**REFINITIV<sup>®</sup>**  
DATA IS JUST  
THE BEGINNING<sup>®</sup>

