Global Economic Crime Survey 2022: UK findings

May 2022

pwc

Contents

Foreword

The past few years have seen a significant degree of disruption and change to the way business is being done, and to the way people work. As organisations face up to the mounting environmental, financial and societal pressures now confronting them, they need a panoramic view of their risk landscape. This is key to building the resilience and confidence needed to navigate this uncertainty, and act boldly and purposefully in pursuit of growth. Fraud risks are an increasingly important component of this risk landscape: economic crimes can be devastating when they hit organisations at scale, in terms of both direct and indirect costs and reputational damage.

Fran Marwood
Head of Digital &
Forensic Investigations

Our 2022 Global Economic Crime Survey (GECS) was conducted before the start of the war in Ukraine. Some responses within this report may have been different if they had been collected weeks later. But while certain risks and disruptions have been heightened, on the whole the trends and dynamics driving the survey responses continue to be topical.

Looking at the UK findings and trends emerging in the 2022 GECS survey, my main reflection is that they are clearly driven by the impacts of the disruption we have seen globally. The importance of evolving and complex risk areas, such as supply chain, and Environmental, Social and Governance (ESG) activities, has risen rapidly, requiring organisations to innovate in how they monitor and manage risk, especially through the use of technology.

In light of the increased levels of disruption, and the fact that more UK organisations have experienced fraud than in our previous survey, I was especially surprised to see a decline in some types of fraud and economic crime, such as cybercrime, bribery, and accounting/financial statement fraud. From discussions with our clients, I believe that some of the trends we have seen are temporary, with, for example, instances of fraud and misconduct remaining undiscovered as traditional controls and corporate culture have evolved during the pandemic. My other, more encouraging, observation is that, in some cases, incidence of these economic crimes is down due to the investment organisations have made in designing and implementing effective compliance programmes, cyber defences and fraud prevention controls.

The overall message for organisations? With fraud now a greater and more costly threat than ever before, and the risk landscape continuing to undergo constant change, it is vital to consider your organisation's readiness to address the challenge. This includes investing in the right resources and effective fraud-fighting measures, and acting quickly and decisively when economic crime is encountered. Fail to take these steps, and you could end up counting the cost.

Our UK headline findings at a glance

With almost two in three of our UK respondents reporting a fraud in the past 24 months, what types of fraud are occurring, who is perpetrating the crimes, and how are they being detected?

What does fraud look like?

of UK respondents experienced fraud, compared to 46% globally (and 56% in UK 2020) (second only to South Africa)

Top five types of fraud reported by UK respondents

Cybercrime
32%
2020: 42%

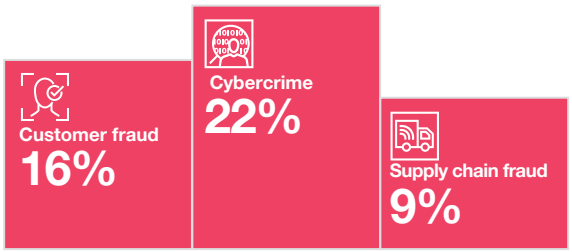
Customer fraud[1]
29%
2020: 33%

Human resources fraud[2]
22%
2020: 24%

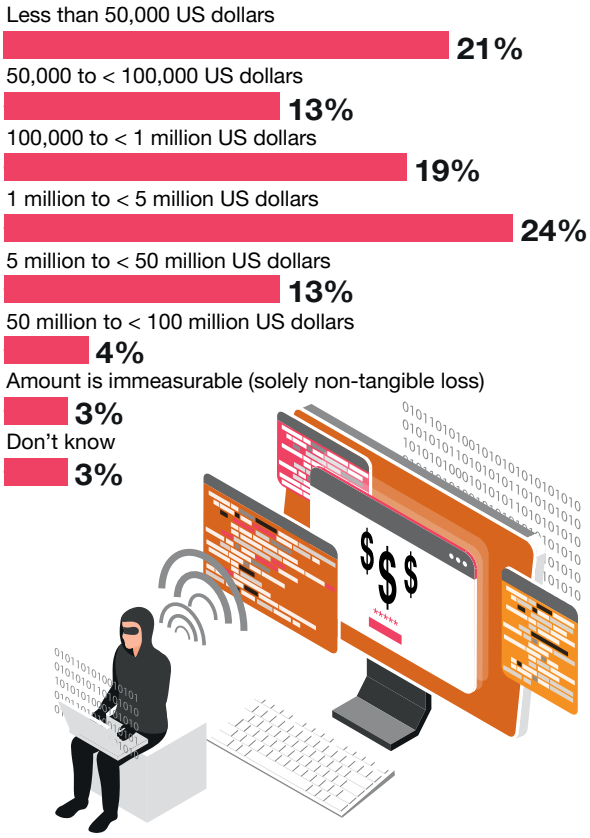
Supply chain fraud
19%
NEW for 2022 N/A

Money laundering and terrorism financing[3]
18%
2020: 13%

Top three most disruptive types of fraud



Total $ lost through fraud in the past 24 months



[1] Customer Fraud is fraud against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others (e.g. mortgage fraud, credit card fraud).
[2] Human Resources fraud is fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work and recruitment (i.e. hiring friends and/or relatives, hiring unqualified individuals, falsification of documents etc).
[3] Money Laundering and Terrorism Finance cover actions intended to conceal or legitimise the proceeds of crime by disguising their true origin, thereby making illegally-gained proceeds appear legal. Can also refer to funds used to finance terrorist groups or acts.

Who is committing fraud and how is it detected?

Who was the main perpetrator?

External
51% vs global 43%

Internal
31% vs global 31%

Collusion
18% vs global 26%

Top five external perpetrators

1 Customer
2 Hacker
3 Vendor / supplier
=4 Organised crime
=4 Competitors

How was the most disruptive/serious crime/fraud initially detected?

Executive summary

Since we published our last GECS report in February 2020, we have seen levels of disruption across the world that we could not previously have imagined. The result has been considerable uncertainty and stress for individuals and organisations – with one impact of the widespread disruption being rising fraud. In the UK, 64% of respondents have experienced fraud, corruption or other economic/ financial crime within the past 24 months, a substantial increase compared to 56% in 2020, and 50% in 2018. This is higher than the global rate of 46%, and second only to the rates seen in South Africa.

In addition to the increased prevalence of fraud in the UK, our survey shows that new fraud risks are evolving. This year we have reflected the heightened challenges in relation to supply chain fraud, and have included this as a separate category for the first time.

The constant evolution of the fraud landscape means that a static model for detecting and preventing fraud simply cannot keep pace. We have always championed the use of technology in the prevention and detection of fraud, when working with our clients and in analysing the survey results, but never has this been more important than today. Such tools are key, for example, in control frameworks that address changes in organisations' working practices, with remote and hybrid working now the norm.

What does this change in working location mean for organisations' ability to create an open culture, where people who see inappropriate behaviour are able to report incidents? Does the physical distance from their teams cause a change in some individuals' mindset, where they may rationalise decisions differently, or are better able to exploit vulnerabilities? And how does the switch to remote and hybrid working impact those controls that previously required physical interactions, but which have been amended or automated to accommodate new working practices?

Alongside the disruption caused by socio-political factors, developments in the UK regulatory landscape are changing how organisations based in the UK seek to address the fraud risks they face. Two good examples include the potential requirement for Directors to report on the actions they have taken to prevent and detect material fraud proposed by the department for Business, Energy and Industrial Strategy (BEIS) in the consultation on 'Restoring trust in audit and corporate governance' (BEIS consultation), and the recent Economic Crime (Transparency and Enforcement) Act 2022 (Economic Crime Act).

The ways in which fraud has been identified also provides interest: the amount of fraud detected via social media (6%) and investigative journalism (3%) demonstrates the continued public interest in this area. Separately, whilst there are encouraging trends around the use of technology and data in fraud detection, the continued reliance on more routine activities to detect such incidents – such as routine internal audits (15%) and corporate culture (whistleblowing / tip-off / confession) (10%) – suggests that there is scope to make greater use of more proactive detection methods.

Our analysis of the UK findings has identified five key trends that stand out in respect of both fraud frameworks and specific risks.

1 Fraud risk and maturity

We explore the impact of disruption on the prevalence and different types of fraud and economic crime. Two of the most disruptive crimes (cybercrime and supply chain fraud) are covered in separate sections below.

Other notable shifts compared to our 2020 findings include the downward trends seen in the UK in reported incidents of both bribery and corruption (10% in 2022 vs 25% in 2020) and accounting or financial statement fraud (10% in 2022 vs 26% in 2020). We suspect that these are temporary dips caused by the disruption that organisations have faced, and may reflect a decrease in detection rather than occurrence. However, anecdotally, it is also clear that investments by some organisations in stronger, better designed and implemented compliance programmes and fraud controls have improved defences.

It is therefore particularly significant, and worrying, that at least one third of UK organisations who responded to our survey still do not have a designated risk management function in place (behind the global average). In addition, only one third of UK businesses had wider awareness of its responsibilities for responding to fraud risks outside of the risk management/compliance functions (again, behind the global results).

We believe strongly that organisations need to focus on implementing a targeted, risk-based approach. Only this will enable them to ensure that they are addressing the evolving risks they face adequately, protecting their reputation, and where necessary, ensuring that they are ready to comply with the changes being proposed to relevant guidance and regulation. This includes the strengthened internal controls regimes proposed in the recent BEIS consultation – similar to the US Sarbanes-Oxley rules, which require Directors to attest to the effectiveness of internal controls over financial reporting.

Finally, learning from mistakes, and taking the opportunity to improve fraud prevention and detection when a fraud occurs, is a critical enabler for effective fraud risk management. It was therefore surprising to see that 15% of UK respondents took no remedial actions after identifying misconduct in their own supply chain, and 19% took no action after identifying misconduct in a third party's supply chain.

> Only 40% of UK respondents reported that they have conducted an enterprise wide risk assessment (less than the 45% reported globally)

> The UK exhibits some encouraging trends, especially in comparison to the global findings, concerning the use of technology for suspicious activity monitoring (15% UK vs 13% global)

2 Data and technology in risk management and detection

Technology continues to play a very important role in managing fraud and economic crime risk and detecting breaches. Changes in internal control frameworks over the course of the pandemic have increased the reliance on technology still further. We believe the key to effective prevention and detection lies in bringing together a variety of data sources to gain a holistic view of risk themes and specific transactions.

The UK exhibits some encouraging trends, especially in comparison to the global findings, concerning the use of technology for suspicious activity monitoring (15% UK vs 13% global). However, the UK is behind the curve when it comes to the use of advanced data analytics (4% UK vs 6% global), which shows significant scope for investment in this area.

3 Supply chain risk and resilience

Today's blend of significant disruption, developing regulation and heightened reputational risk makes it more important than ever for organisations to understand who is in their supply chain, and what those parties are doing that could give rise to fraud and integrity related risks. At the same time, organisations are increasingly expected to take responsibility for the conduct and performance of those working in their supply chains, including sanctions risks. Some 19% of UK respondents said they had experienced supply chain fraud – a remarkably high figure for this new category of fraud in our 2022 survey.

Whilst four in five respondents reported that they were confident about their management of supply chain risks, the levels of misconduct and supply chain fraud – as well as challenges reported concerning the visibility of risks and inefficient technology being used to manage the risk – suggest that there is more work to be done in this area.

4 ESG risk

Organisations are experiencing increased focus and public scrutiny around the ESG impacts of their activities. This scrutiny, combined with increasing legal and regulatory requirements, has led many organisations to make public commitments on issues like net zero and the treatment of staff and those involved in their supply chain. The pressure to publish targets, and the shareholder value placed on achieving these (with linkages frequently put in place between meeting those targets and directors' remuneration) creates an environment where organisations are at increasing risk of greenwashing. This is the attempt to convey a false impression of their environmental credentials.

One major consideration here is how organisations can understand and manage the ESG risks that exist within their supply chains, with one in three UK respondents admitting to an inability to monitor or report accurately on the ESG metrics associated with third party partners.

5 Cybercrime

Cybercrime remains the single most pervasive type of fraud facing UK organisations, experienced by 32% of our UK respondents. It's also regarded by those completing the survey, as the most disruptive – cited by 22% of UK organisations – with ransomware being the most prevalent issue encountered. Despite this, surprisingly, we have seen a 10% decline in the overall levels of cybercrime reported by our UK respondents. This may indicate that the significant focus that many organisations have given the topic, and related investment in preventative measures, has proven effective. However, the risks around cybercrime continue to evolve.

What is more, cybercrime can often be a precursor to other types of crime. Given that systems are now more integrated than ever before, there is a major concern that parties in their supply chain or customer base may prove to be the weak links in their cyber defences. 63% of organisations in our 2022 Cyber Security Strategy expect to see an increase in supply chain cyber threats.

> Organisations are experiencing increased focus and public scrutiny around the ESG impacts of their activities

1. Fraud risk and maturity

What trends do we see in the prevalence and types of fraud?

Organisations have faced huge disruption over the past two years. Our 2022 survey clearly shows the impact of this disruption through the increased prevalence of fraud, together with shifts in the key types of fraud being faced by UK organisations.

In the UK, 64% of respondents experienced fraud, corruption or other economic crime within the last 24 months, a substantial rise from the 56% who fell victim in 2020 and compared to 50% in 2018. This is also much higher than the global rate of 46%, and is second only to the rates seen in South Africa. In addition, 51% of the most disruptive incidents of crime/fraud reported by our respondents were committed by external perpetrators (compared to 43% globally). This may suggest that UK organisations are an increasingly attractive target to external fraudsters.

Further insights from the survey include how the types of fraud experienced by our UK respondents compares to the global position, and also how this has changed since our last survey in 2020.

We explore the significance of the trends in cybercrime and supply chain fraud later in this report. Whilst asset misappropriation is a significant issue reported globally, this does not feature in the top 5 for the UK.

Two other notable areas where a decline has been reported by UK respondents in our 2022 results are in relation to incidences of bribery and corruption, and the level of accounting or financial fraud.

What types of fraud, corruption or other economic crime has your organisation experienced in your territory within the past 24 months?

UK 2022 (top five)	UK 2020 (top five)
1. Cybercrime **32%**	**1.** Cybercrime **42%**
2. Customer fraud **29%**	**2.** Customer fraud **33%**
3. Human Resources fraud **22%**	**3.** Accounting/ Financial Statement Fraud **26%**
4. Supply chain fraud **19%**	**4.** Bribery and Corruption **25%**
5. Money laundering and terrorism financing **18%**	**5.** Human Resources fraud **24%**

Global (top five)

1. Cybercrime **37%**

2. Customer Fraud **33%**

3. Asset Misappropriation **25%**

4. Procurement Fraud **20%**

5. Know Your Customer (KYC) Failure[4] **19%**

> Almost two in three UK respondents have experienced fraud, corruption or other economic crime within the last 24 months, higher than the average global rate of 46%, and second only to the rates seen in South Africa.

[4] Know Your Customer (KYC) failures include inadequate controls or measures to verify customer information, resulting in fake or fraudulent activities.

> This year's results in the UK show an increase in the prevalence of frauds perpetrated by third parties, notably customers and suppliers. Money laundering and cybercrime, both typically driven by external third parties, also make the UK top 5

A rise in third party related economic crime

This year's results in the UK show an increase in the prevalence of frauds perpetrated by third parties, notably customers and suppliers. Money laundering and cybercrime, both typically driven by external third parties, also make the UK top 5. Given the levels of disruption in supply chains and financial pressures on customers and other third party groups, this is perhaps an unsurprising, if worrying, development. However, with inflationary, pandemic and other geo-political market risks persisting, these are clear indicators of key focus areas for fraud risk and control investments within UK organisations. We expect to see a corresponding increase in levels of customer, third party and supplier due diligence and risk monitoring activities.

A downward trend in bribery and corruption – or a short-term dip?

Another finding from the UK survey that is worthy of particular mention relates to the incidence of reported bribery, which has decreased to 10% in 2022, from 25% in 2020. A similar decline has been seen in the number of respondents who had lost an opportunity to a competitor who they believed paid a bribe, down to 31% in 2022 from 38% in 2020. In light of our everyday conversations with clients, and the increased bribery risks that might be expected when there are significant pressures in the supply chain, these are intriguing statistics. Could these declines be a function of the dramatic reduction in face-to-face meetings and hospitality over the past two years? Of remote working practices having an impact on detection? Or might they be due to lower levels of activity from a regulatory perspective? It could also be the case that compliance programme investments are paying off. It will be interesting to see how these figures evolve as the world continues to open up post pandemic.

A decrease in incidences of accounting or financial statement fraud – or a temporary decline in successful detection?

There has been a significant drop in the level of accounting or financial statement fraud since the 2020 GECS survey, with just 10% of UK respondents experiencing this in the past 24 months, compared to 26% in 2020 and 17% globally in 2022. The disruptive impact of accounting fraud has also seen a significant decrease since 2020, with only 3% of UK respondents viewing this as the most disruptive/serious type of fraud, down from 15% in 2020.

Our experience suggests that instances of fraud might be expected to increase given the effects of external disruption. Controls may not have been operating at full efficiency, and governance and oversight may have been less effective (which could have been the case due to control framework changes made to accommodate home working). Incentives and pressures on individuals could also be argued to have been higher due to a perceived need to demonstrate their value to their organisation during a time of economic stress. Could it be the case that it is only the detection of accounting fraud that has decreased, rather than the occurrence? And, similar to the reporting of bribery and corruption, will we see a rebound as we go forward?

What trends do we see in risk management?

Almost a quarter – 24% – of UK respondents estimate their organisation's loss due to incidents of fraud, corruption or other economic/financial crime over the last 24 months as between US$1 million and US$5 million. This reinforces the fact that the financial impact on organisations can be substantial.

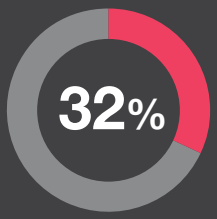
Perhaps surprisingly, one third of UK organisations responding to our survey do not have a designated risk management or compliance function in place. This is behind the global average (32% vs 26% globally). The UK is also behind the global average in terms of the number of organisations with wider awareness of their responsibilities for responding to fraud risks outside of the risk management/compliance functions (34% vs 43% globally).

In addition, only 40% of UK respondents reported that they have conducted an enterprise wide risk assessment (less than the 45% reported globally).

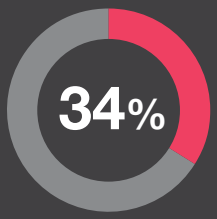
That said, a positive trend is that UK organisations are recognising the need for investing in risk management systems, with 54% of UK respondents indicating their risk management functions have grown over the past 24 months.

We expect that the BEIS consultation and ensuing likely increase in corporate governance responsibilities will only serve to intensify the focus on the role of a fraud risk management function, with directors of Public Interest Entities perhaps being held to a greater level of accountability for their actions to prevent and detect material fraud.

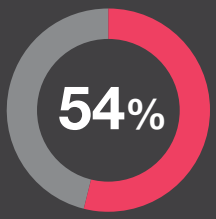
We are increasingly finding boards probing management more about how fraud risk is managed, with an increased focus on three actions in particular: conducting a risk assessment; promoting a strong corporate culture and values; and ensuring that appropriate control activities, including those relating to fraud detection, are in place and operating effectively.



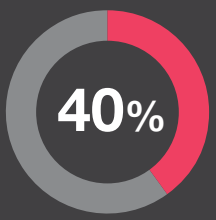
of UK respondents do not have a designated risk management/ compliance function in place



of UK respondents have a wider awareness of their fraud risk management responsibility outside of the risk management/ compliance function



of UK respondents have risk management functions that have grown in size over the past 24 months



of UK respondents reported that they have conducted an enterprise wide risk assessment (less than the 45% reported globally)

Adopting a targeted, risk-based approach and closing the gap when fraud is detected

Against a background of constant change in the fraud landscape, it is increasingly difficult for organisations to ensure they have everything covered across the five key components of a fraud risk management framework. We explore the key elements of a fraud risk management framework and a number of practical considerations in our 'Restoring trust through enhanced fraud risk management' paper. The five key components are:

Fraud governance

Corporate governance failures are behind many high profile corporate frauds. Protected organisations have a strong governance and reporting structure, with clearly defined roles and responsibilities around fraud risk.

Fraud risk assessment

A comprehensive risk assessment is fundamental to capturing key fraud risks, assessing the impact they have on the organisation, and key controls in place to prevent and detect instances of fraud.

Fraud prevention

Well designed and operationally efficient controls that protect an organisation from internal and external fraud.

Fraud detection

The processes and systems that actively look for fraud in key risk areas, enabled by innovative technology.

Fraud response

The organisation's ability to rapidly and effectively investigate fraud and trace assets, individuals and networked relationships.

To protect an organisation as effectively as possible against fraud, we believe that a targeted, risk-based approach is the best course of action, particularly where there are challenges around limited resources and investment. A thorough risk assessment, that is refreshed regularly, is critical here. It means that time, resources, and technology investment are tailored to target those fraud risks which pose the biggest threat.

Another critical enabler for effective fraud risk management is learning from mistakes and taking the opportunity to improve fraud prevention and detection when a fraud occurs. In order to be effective, this needs different parts of organisations to collaborate, which is not always easy to implement. It was therefore surprising to see that 15% of UK respondents took no remedial actions after identifying misconduct in their own supply chain, and 19% took no action after identifying misconduct in a third party's supply chain.

15%

of UK respondents took no remedial actions after identifying misconduct in their own supply chain, and 19% took no action after identifying misconduct in a third party's supply chain

2. Data and technology in risk management and detection

Why is the need to use technology in fraud risk management and detection higher today?

The constant evolution in the fraud landscape means that a static model for detecting and preventing fraud simply cannot keep pace.

Organisations have had to place greater reliance on technology at a time when some other controls have been weakened, or lost entirely, due to changing working practices and organisational change over the course of the pandemic. At the same time, the reduction in checks and balances throughout the working day in time spent with other colleagues may be bringing its own risks and temptations that link back to the fraud triangle.

We have always championed the use of technology in the prevention and detection of fraud when talking to clients and analysing the survey results, but never has this been more important than today. In this regard, new questions included in our survey this year point to some encouraging trends in recognising the importance of technology, including in emerging risk areas such as ESG, with 67% of UK respondents reporting they are leveraging technology to monitor, track and report on ESG metrics (vs 60% globally). However, there is still progress to be made.

> We have always championed the use of technology in the prevention and detection of fraud when talking to clients and analysing the survey results

> While the UK seems to be at the forefront when it comes to suspicious activity monitoring (15% UK vs 13% Global), it is behind the curve on using advanced data analytics (4% UK vs 6% globally)

Is the deployment of technology resulting in better prevention and detection of fraud?

Our results show that organisations are using technology in a number of ways.

For example, they are looking to detect the most disruptive incidents of fraud or economic crime through measures including suspicious activity monitoring (15%, up from 11% in 2020), corporate security (12%, up from 7% in 2020) and advanced data analytics (4%, no change from 4% in 2020).

While the UK seems to be at the forefront when it comes to suspicious activity monitoring (15% UK vs 13% Global), it is behind the curve on using advanced data analytics (4% UK vs 6% globally). In addition, the continued reliance on more routine activities to detect such incidents – such as routine internal audits (15%) and corporate culture (whistleblowing / tip-off / confession) (10%) – suggests that there is scope to make greater use of more proactive detection methods.

How can technology be used more effectively?

Organisations have access to a wide array of tools and data sources to support fraud prevention and detection efforts, and we believe the key to effective prevention and detection lies in bringing together a range of different data sources to identify patterns and anomalies more effectively.

We see innovative organisations using a range of data sources in their ongoing monitoring, extending across operational systems, employee surveys, communication data and external data sets such as company intelligence, social media, news or dark web data.

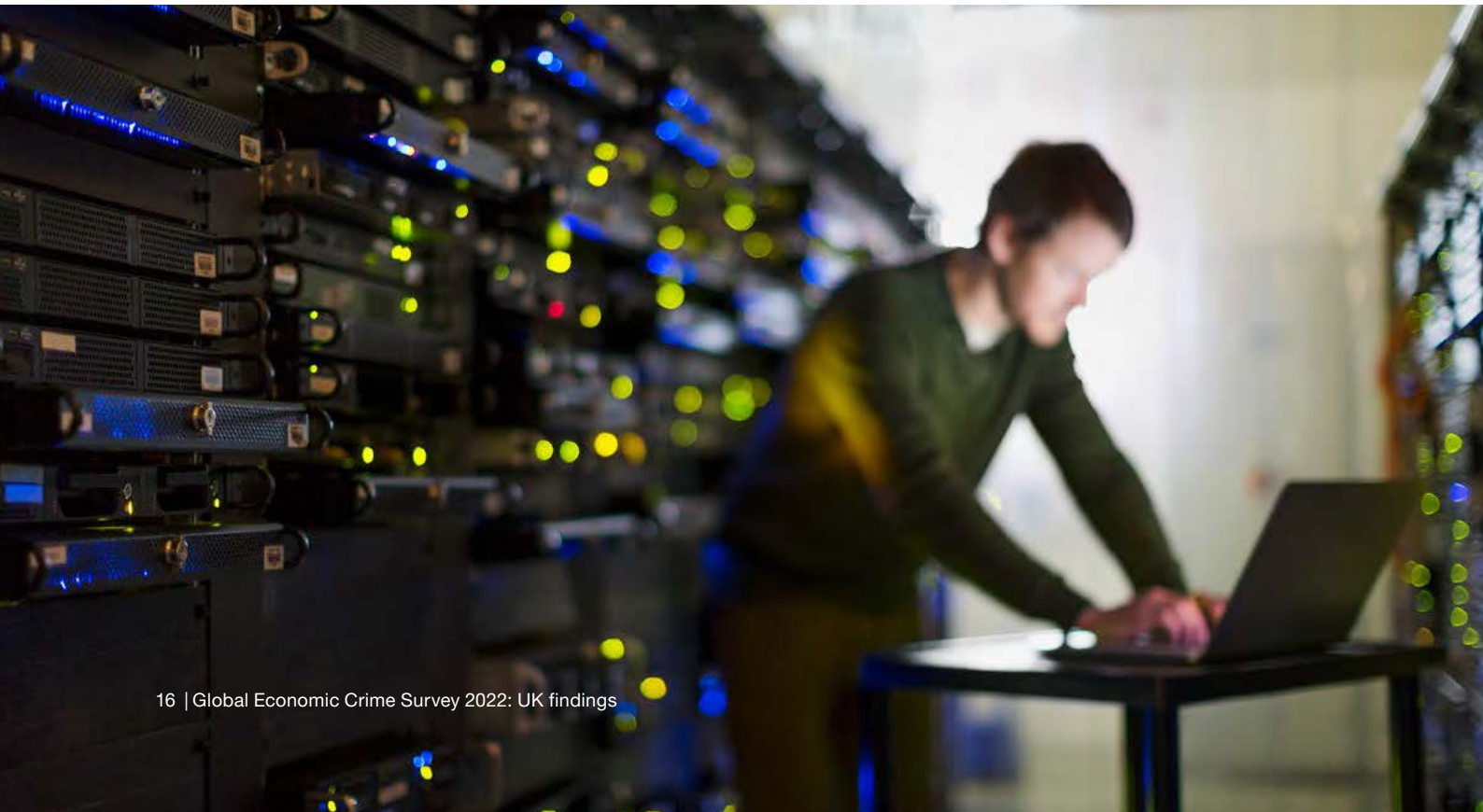
Organisations using basic analytics techniques may experience a high number of false positives, thus making it harder to pinpoint fraud. Visualisation and machine learning are helping greatly to tackle this issue. Combined with tools like natural language processing and entity resolution, artificial intelligence can be an effective method of identifying matches between different datasets and has proven increasingly effective in ranking riskier transactions to aid prioritisation by the organisation.

Examples might include identifying customers who have applied for multiple loans using slightly different names or addresses, or identifying suppliers who match companies that are sanctioned.

Traditional techniques are still highly effective and should not be discounted. But our experience confirms that there are significant benefits to be reaped from layering newer approaches on top of rules-based testing.

“

Organisations using basic analytics techniques may experience a high number of false positives, thus making it harder to pinpoint fraud



3. Supply chain risk and resilience

Why is supply chain risk evolving so quickly?

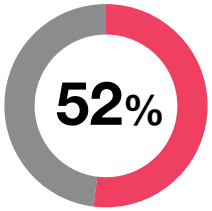
A shortage of goods and materials in the supply chain is among the more obvious issues that spring to mind when thinking of supply chain risk.

This brings with it risks around disruption to supply chain management, partnering with new third parties, contracting changes, market entry/exit, financial distress and operational delays. In addition, the increasing remit of global sanctioned entities has heightened the need to know who you're doing business with, and has increased the need for sophisticated intelligence solutions and third party compliance programmes. In addition, organisations are also being expected increasingly to take more responsibility for the conduct and performance of their supply chains, at a time when those supply chains are lengthening and becoming more complex.

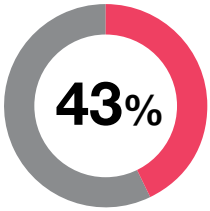
We chose supply chain risk as an area of focus for our survey in 2022, following a huge increase in this type of fraud affecting our clients.

What our clients have been telling us is corroborated by the survey results. They show that supply chain fraud (defined in this survey as fraud or corruption related to the production or distribution of a company's goods or services) was experienced by 19% of our UK respondents (18% globally) in the past 24 months. In addition they show that broader supply chain misconduct was experienced by 52% of UK respondents (44% globally). The megatrends faced by organisations may be boosting the risks of opportunistic fraud in this area: 30% of our UK respondents reported new (13%) or increased (17%) risk of supply chain fraud as a result of the pandemic.

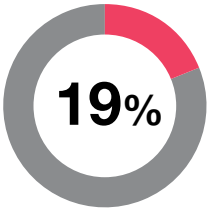
Upcoming regulations, such as the EU Corporate Sustainability Reporting Directive and UK Economic Crime Act, will increase the supply chain monitoring, sanctions screening and reporting requirements for many organisations. We may see UK-based organisations following a similar monitoring and reporting approach to that adopted by the EU, as a result of pressure from relevant stakeholders.



reported identifying misconduct in their supply chain (compared to 44% globally)



reported identifying misconduct in the supply chain of a third party (compared to 38% globally)



reported experiencing supply chain fraud in the past 24 months

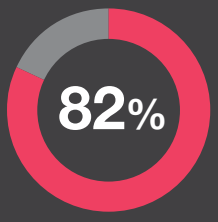
Are supply chain risks being managed effectively?

The majority of UK respondents in our study reported that they manage their supply chain risks proactively (82%) and/or effectively (83%), higher than the global results (78% and 77% respectively).

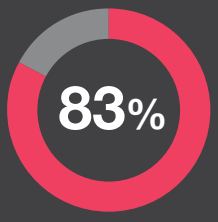
In light of these responses, the gaps UK respondents identified as influencing their ability to manage supply chain risks may appear surprising, with 70% of UK respondents identifying a lack of visibility of risks (vs 61% globally) and 66% reporting inefficient technology or processes to identify and manage supply chain risks (vs 60% globally). It may be that the increased focus on supply chain management is still at an early stage, and therefore that some organisations are showing a degree of overconfidence given the unknown unknowns that are out there.

What is clear overall is that many organisations are experiencing challenges when it comes to managing their supply chains. A holistic approach to risk management is essential to increase resilience and ensure all evolving and emerging risks are addressed. While technology is playing an ever greater role in improving visibility into supply chain risks, achieving the fullest possible visibility requires a multidisciplinary team approach.

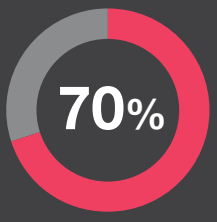
We are seeing increasing use of third party portals for risk assessment purposes, with examples including our own Third Party Tracker tool, as well as increased use of sophisticated intelligence based solutions being used to address specific risk areas such as sanctions tracking.



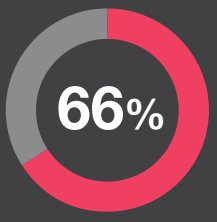
agreed or strongly agreed that they proactively managed their supply chain and risks



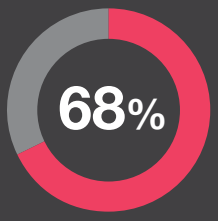
agreed or strongly agreed that they effectively manage supply chain risk



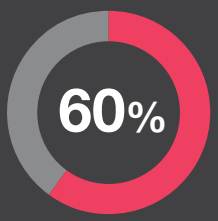
identified a lack of visibility of risks throughout the supply chain



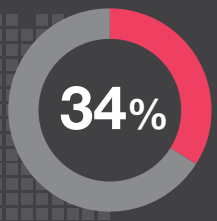
identified inefficient technology or processes to identify and manage supply chain risks



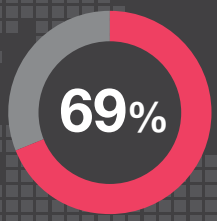
(vs 57% globally) believed that onboarding suppliers at pace leads to an inability to ensure all risk management elements have been addressed



of respondents do not have a fully implemented company-wide risk assessment



UK respondents felt they had an inability to accurately monitor or report ESG metrics of third party business partners



UK respondents were at least somewhat concerned about manipulation/fraud of ESG reporting by employees within their organisation

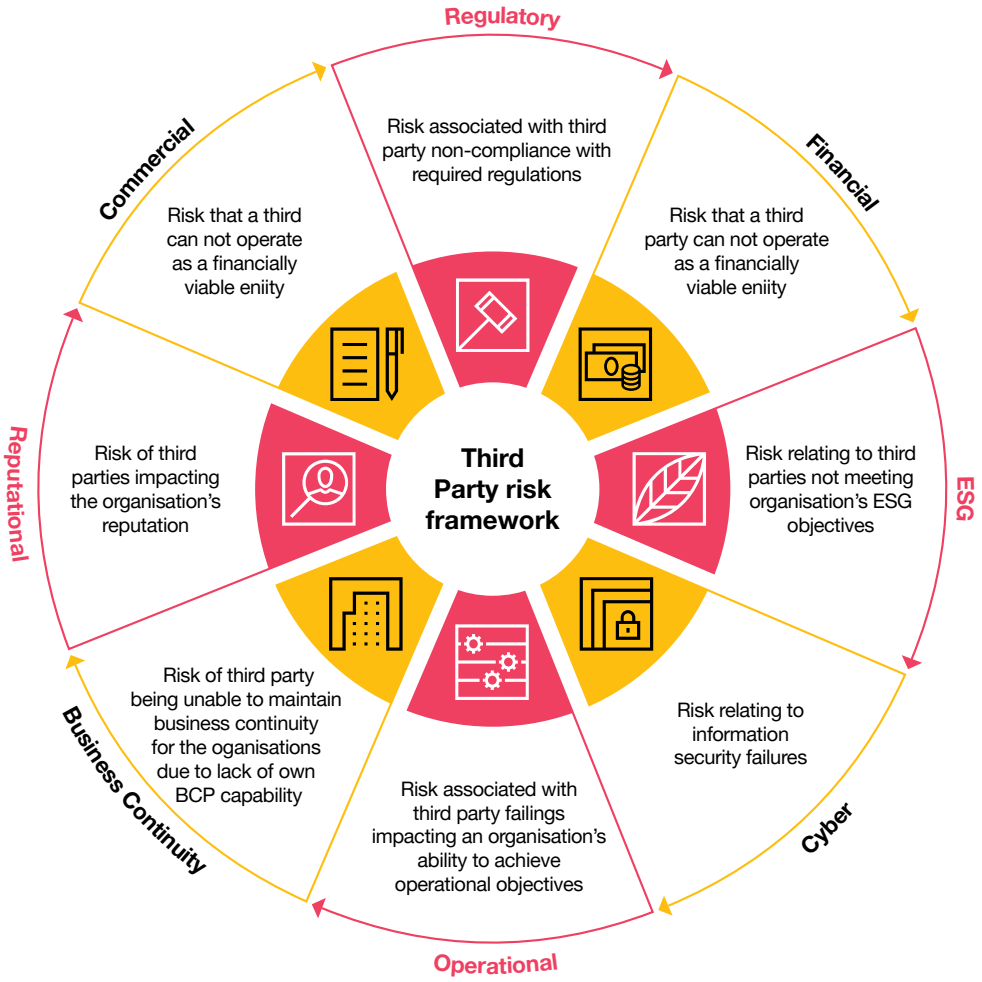
How can you fully understand the complexity of your supply chain risks?

Recent developments, such as significant sanctions, and the impacts of the pandemic and Suez canal disruptions on the manufacturing and movement of goods, have served to highlight the importance of knowing who is in your supply chain and where they operate.

The ability to map the whole supply chain is good practice if an organisation is to fully understand the risks it faces. For example, instances of greenwashing at any point in an organisation's supply chain have the potential to negatively impact its reputation, as do allegations relating to modern slavery or hidden environmental issues.

At the heart of effective supply chain risk management in any organisation must be an organisation-wide risk assessment and framework, from which mitigating defences can be deployed. We find it concerning that only 40% of our UK respondents (compared to 45% globally) reported having an organisation-wide supply chain risk assessment fully implemented.

The chart below shows a sample third party risk framework, which can serve as a helpful tool in understanding, mapping, and monitoring an organisation's supplier and wider third party risks. Organisations then need to think about how they can build their resilience to mitigate and manage these risks with confidence, ideally using a data-driven approach, and deploying contractual levers with targeted interventions for higher-risk suppliers.



4. ESG risk

43%

of UK respondents (vs 35% globally) indicated that a lack of ownership of ESG in their organisation was one of their top three concerns

How has the increased focus on ESG impacted fraud and fraud risk?

The profile of ESG issues continues to increase, with growing scrutiny of organisations' conduct in the public domain, accompanied by an increasing trend towards greater non-financial reporting requirements and regulations.

Highly publicised events such as COP26, together with an increase in mandatory reporting (the UK government became one of the first to mandate reporting of Task Force on Climate-Related Financial Disclosures (TCFD)) are already having an effect on monitoring and reporting requirements. In the future, these requirements are likely to become even more stringent. Indeed, 70% of our UK respondents said they were at least somewhat concerned by upcoming regulations related to ESG reporting standards.

New areas of risk, such as ESG, are often accompanied by uncertainty around responsibility and how to manage the risks themselves. Historically, there has been a lack of consensus on where responsibility for managing ESG risks lies within organisations, with these being owned by different functions in different organisations. However, in light of the increasing focus on ESG risks, many organisations are starting to seek a more joined up approach – or at least clearer ownership. Notwithstanding this shift, 43% of UK respondents (vs 35% globally) indicated that there was a lack of ownership of ESG in their organisation.

What is greenwashing – and what to look out for?

Greenwashing is an attempt to capitalise on the demand for environmentally conscious products and services by overstating green credentials that are not supported by real underlying sustainability related activities.

Whilst often a deliberate strategy, greenwashing can also happen inadvertently when not enough attention is paid to the actions and compliance of the organisation itself, or the third parties in its supply chain. More than two thirds – 69% – of our UK respondents were at least somewhat concerned about manipulation/fraud of ESG reporting by their employees, and 66% were concerned about manipulation/fraud of ESG reporting by third parties they rely on, mirroring the global findings.

There are many factors at play in relation to greenwashing, or the attempt to convey a false impression of their environmental credentials. For example, stakeholders are increasingly expecting organisations to publish their ESG targets, whether these be around environmental metrics or information about the organisation's position with respect to human rights and modern slavery, and whether they relate to the organisation's own activities or also include those of the wider supply chain.

This trend increases the risk of greenwashing, as organisations may rush to publish targets without formulating a plan for how these will be achieved. A desire to show positive movement against published targets may provide an additional incentive to manipulate results.

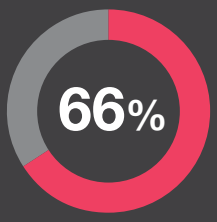
This will become even more relevant if director remuneration is tied to the ESG targets, or if organisations also have sustainability-backed loans, which essentially offer a lower interest rate if they achieve certain ESG KPIs. As our 2022 Global CEO Survey shows, this is the case for one in three CEOs of the largest organisations, where their remuneration is linked to their performance in areas like reducing greenhouse gas emissions.

How confident do organisations feel in managing ESG risks

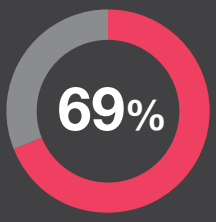
66% of our UK respondents (vs 55% globally) reported that they are able to monitor the accuracy of their third party partners' ESG performance.

In addition, almost four in five UK respondents believe that they have processes in place to identify and manage potential risks with respect to ESG reporting (69% for environmental, 71% for social and 85% for governance). Having discussed ESG risks with our clients, we believe that those organisations who are at an earlier stage in their ESG journeys may be more confident at first glance, but might be showing a degree of overconfidence given unknown unknowns, similar to the situation with supply chain risk.

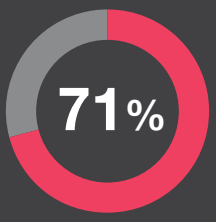
A further key challenge is around how to accurately monitor the ESG performance of third party partners. Unless an organisation can do this, it is difficult for it to identify potential breaches which could have just as significant a reputational impact as a breach within the organisation itself. This should be worrying for the 34% of UK respondents who stated that they did not have this capability. We know that even organisations who are comfortable that they understand the risks associated with their Tier 1 suppliers are much less confident concerning the risks posed by Tier 2 and below. This is just one example of where the supply chain risks discussed in the previous section overlap with ESG risks, serving to underline the importance of considering fraud and integrity risks holistically across the organisation.



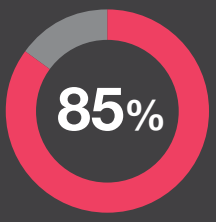
believe they are capable of monitoring the accuracy of their third party business partners' ESG performance



believe that they have processes in place to identify and manage potential risks with respect to environmental reporting



believe that they have processes in place to identify and manage potential risks with respect to social reporting



believe that they have processes in place to identify and manage potential risks with respect to governance reporting

5. Cybercrime

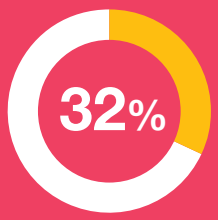
Why does cybercrime remain so high on the list of priorities?

The accelerated shift to online ways of doing business and working prompted by the pandemic is driving more digital transformation than ever before. But it also creates new opportunities for cyber criminals.

Almost one third – 32% – of UK respondents noted that their organisation has experienced cybercrime in the past 48 months. Cybercrime continues to be highly disruptive, with 22% of UK respondents agreeing it to be the most disruptive and serious type of fraud risk with respect to the impact on their organisation. This mirrors the messages from our PwC's 25th Annual Global CEO Survey, where 49% of CEOs stated they were most concerned about cyber risks.

Zeroing in on the various types of cybercrime, ransomware (as discussed in our recent human-operated ransomware whitepaper) remains by far the most prevalent issue that we see organisations contending with across all sectors and geographies. PwC's recent study 'Cyber Threats 2021: A Year in Retrospect' reported that the number of ransomware victims who had their data exposed on leak sites had almost doubled to 2,435 since our 2020 research.

However, whilst awareness and the perceived impact of cybercrime remain high, it is interesting to note that the number of respondents saying they had experienced cybercrime has fallen by 10% since our 2020 results. Why would this be? We believe it might provide an indication that the recent investments in preventative measures are starting to pay dividends.



UK respondents noted that their organisation experienced cybercrime in the last 48 months

Cybercrime was identified by our UK respondents as the most disruptive/ serious type of fraud risk with respect to the impact on their organisation

> Over the past two years, we have seen ransomware threat actors operating increasingly on a double-extortion model

Why should we be concerned about cybercrime being a precursor to other types of crime?

Cybercrime – whether involving initial phishing or exploitation of vulnerabilities, or the deployment of ransomware – is in many instances a precursor to other types of crime.

Over the past two years, we have seen ransomware threat actors operating increasingly on a double-extortion model: one where they do not just require the victim to pay a ransom to decrypt their systems, but also pressure them into paying the ransom by stealing confidential information and threatening to leak it. The information involved may be intellectual property, employee data, or other information assets that can be leaked into the public domain (with subsequent regulatory impacts), or sold on to other criminals for different purposes.

Payment of the ransom demand is no guarantee that data will be recovered, or that exfiltrated data will not be leaked or sold to third parties. Additionally, ransom payments help to fund the continued activity of cyber criminals. If your organisation does fall victim to a ransomware attack, we recommend that you work closely with suitable external counsel to investigate the legality of any potential payment, particularly with regard to US sanctions.

> Organisations should remain alert to the cyber threats presented by their intermediaries and third parties

How is cybercrime changing and evolving?

While the established types of cybercrime have continued to occur, a significant number of respondents have also experienced new (18%) or increased (25%) cybercrime risk as a result of the pandemic. This is unsurprising due to organisations' increased digital presence and reliance on online platforms.

The key question remains: how are organisations ensuring that they remain alert to the changes in risks associated with global events – and how can they manage these shifts and build the resilience to prevent or withstand attacks? This question may be particularly relevant to smaller organisations, whom we see being targeted increasingly due to their more limited preventative and detective measures.

However, it is also worth noting that for some of the most active ransomware threat actors, a victim's level of revenue is an important factor when deciding whether to proceed with a ransomware attack. Ransomware threat actors might initially target many organisations to see where they are able to breach defences, but then narrow their approach to only attack those that are more likely to pay a ransom or fund a bigger payout.

Organisations should remain alert to the cyber threats presented by their intermediaries and third parties. With today's systems being more connected than ever before, the question becomes: how can you be sure that the next attack won't be channelled via your supply chain or customer base?

Contact us

Claire Reid
UK Forensics Services Leader

+44 (0)7734 607594
claire.reid@pwc.com

Mark Anderson
Digital & Forensic Investigations Partner (Supply Chain Risk and Resilience)

+44 (0)7770 921256
mark.r.anderson@pwc.com

Fran Marwood
Head of Digital & Forensic Investigations

+44 (0)7841491400
fran.marwood@pwc.com

Laura Middleton
Digital & Forensic Investigations Director (ESG)

+44 (0)7730 067252
laura.middleton@pwc.com

Rachael Joyce
Digital & Forensic Investigations Director

+44 (0)7841 569306
rachael.joyce@pwc.com

Stuart McMeechan
Digital & Forensic Investigations Director (Analytics in Fraud Detection)

+44 (0)7483 422762
stuart.mcmeechan@pwc.com

Jonathan Holmes
Digital & Forensic Investigations Partner (Fraud Risk Management & ESG)

+44 (0)07809 755613
jonathan.holmes@pwc.com

Ronan Magee
Digital & Forensic Investigations Director (Cybercrime)

+44 (0)7715 211319
ronan.magee@pwc.com

pwc.co.uk

SPS Design RITM8264321 (05/22).