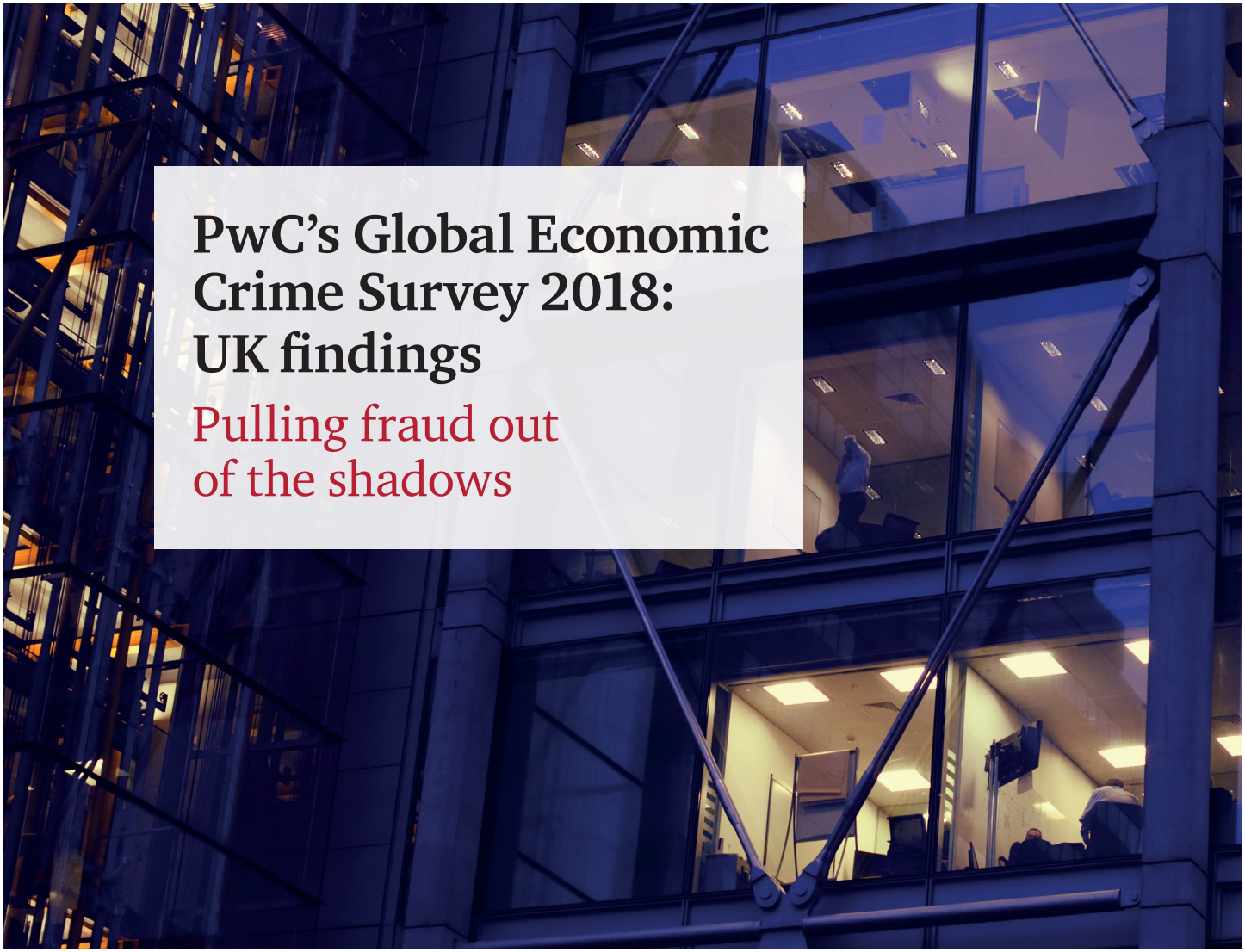
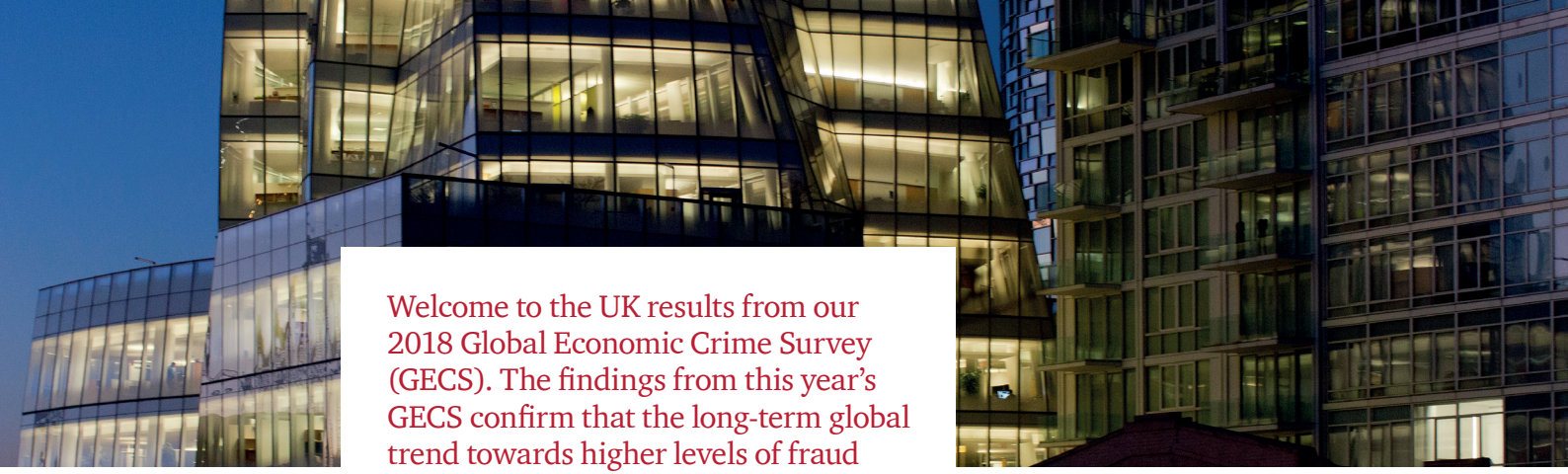


PwC's Global Economic Crime Survey 2018: UK findings

Pulling fraud out of the shadows

pwc

www.pwc.co.uk/gecs



Welcome to the UK results from our 2018 Global Economic Crime Survey (GECS). The findings from this year's GECS confirm that the long-term global trend towards higher levels of fraud is continuing, and clearly show the destructive impact that this rising tide of economic crime is having on businesses.

Fran Marwood
Investigations Partner,
Forensic Services
PwC UK

According to our study, nearly a quarter of frauds occurring in the UK over the past two years resulted in a loss of over $1m (£700,000). The direct costs are increased still further by the burden of investigating and remediating after a fraud, and businesses are feeling the resulting impact on their reputation, brand, employee morale and relationships with business partners.

Experience shows that times of uncertainty often create new openings for fraudsters to exploit gaps or weaknesses in controls, and it's significant that over a quarter of respondents to our survey felt that the current geopolitical climate would lead to more opportunities for people to commit fraud. As such findings underline, it's now more crucial than ever that businesses understand the fraud risk landscape and all the possible avenues of attack.

Rising usage of digital technologies is a futher factor. With businesses relying ever more heavily on the benefits of technology and the use of data, it is hardly surprising that our survey has revealed yet another rise in the number of UK organisations experiencing cyber attacks in the past two years. Our survey showed that cybercrime is the most commonly experienced fraud, overtaken by asset misappropriation for the first time. Yet we have also seen increases in the number of organisations reporting other types of fraud, notably bribery and corruption and procurement fraud, despite the overall level of UK businesses experiencing fraud falling from 55% in 2016 to 50% in 2018. It is also apparent that the UK is lagging behind much of the rest of the world in harnessing technology to prevent and detect fraud.

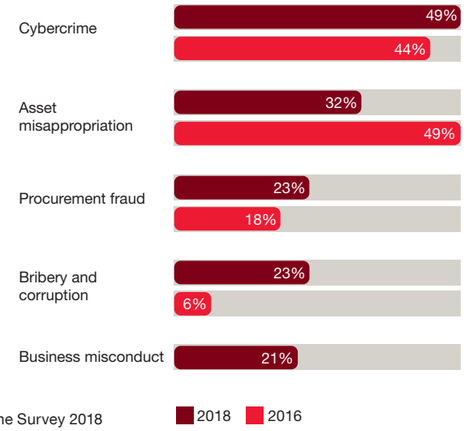
In this year's report, we use the UK results from GECS to explore three key themes:

- How do you make the best choices around preventing and detecting fraud?
- How can you focus your resources and use technology more effectively?
- What do the results say about UK businesses' approach to bribery and corruption?

Know what fraud looks like

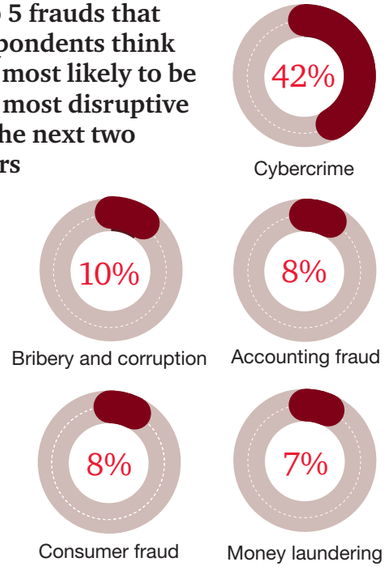
50% of UK respondents reported experiencing economic crime in the past 24 months, in line with the global average of 49% and a reduction in the UK from 55% compared to 2016.

Top 5 types of reported fraud in 2018:

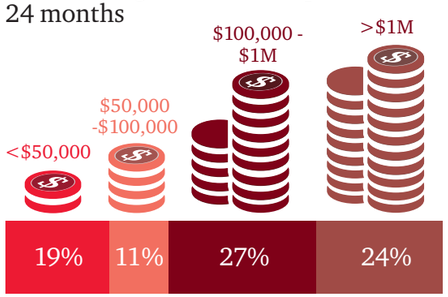


Source: Global Economic Crime Survey 2018

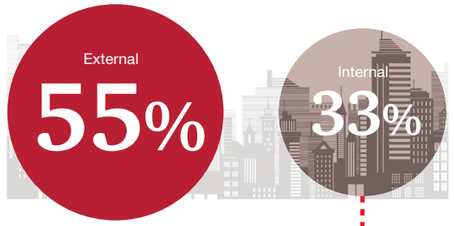
Top 5 frauds that respondents think are most likely to be the most disruptive in the next two years



$ lost through fraud in the past 24 months



55% of frauds were committed by external perpetrators (Global: 40%). **33% were committed by internal perpetrators** (Global: 52%)



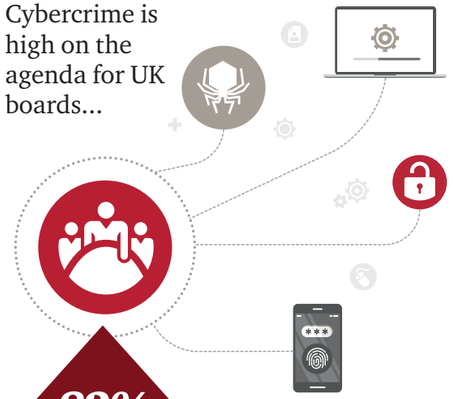
remaining respondents either don't know or prefer not to say

Half the frauds committed by internal perpetrators were committed by senior management, up from 18% (in 2016)

+32%

45% of respondents felt that the main reason was the opportunities presented to the individual.

Cybercrime is high on the agenda for UK boards...

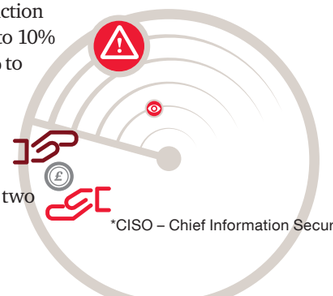


...with **82% of CISO's* reporting into the board** (compared to 61% globally)

19% of frauds were detected through fraud risk management and **15%** were detected by internal audit.

The success of suspicious transaction monitoring (from 22% in 2016 to 10% in 2018) and data analytics (8% to 1%) has declined in the UK.

24% have been asked to pay a bribe in the last two years – up from 5% in 2016.



*CISO – Chief Information Security Officer

Making good choices:

How well do you understand your fraud risks?

24%

of frauds saw the victims lose more than

$1M (£700,000)

Fraud imposes significant costs on UK business. Half of the respondents to our survey reported that they have experienced fraud in the last two years, similar to the global level – and our experience suggests that many more may have fallen victim to fraud without realising it.

Our study also shows that the incidence of fraud is continuing to trend upwards over time, both in the UK and globally.

These findings are borne out by frequent media reports covering the full spectrum of fraudulent activity, ranging from the latest cyber scams against businesses and consumers, to corporate executives facing serious charges.

The continuing flow of frauds takes a heavy financial toll on the businesses affected. Over half of the most disruptive frauds in the UK resulted in losses of over US$100,000 (£70,000), while some 24% of frauds saw the victims lose more than US$1m (£700,000). These are significant costs both to UK business and the wider economy. Also, importantly, the proceeds often end up in the hands of organised criminals, funding a range of activities from terrorism to human trafficking.

Organisations face potential attack from multiple angles – customers, suppliers, cyber criminals, organised crime, employees, and many more.

The range of fraud also continues to expand and, for every threat and risk that an organisation identifies and manages today, new risks arise as it develops and grows its activities over time. Experience shows that times of economic uncertainty and change, with businesses expanding into new global markets, holding and utilising more data, and implementing new technologies, give rise to increased opportunities and pressure on individuals to commit fraud.

27% of our respondents expect that the geopolitical environment will result in increased economic crime in the next two years, and only 9% are expecting a decrease (compared to 18% globally).

Business conduct and misconduct

This year we have included a new category of fraud: business conduct/misconduct. We define this as frauds where the company is the perpetrator, with the criminal activity typically affecting customers or suppliers through activities such as deliberate overcharging. This type of crime affected 21% of those respondents in the UK who reported experiencing a fraud in the last two years.

Both globally and in the UK, we have also seen a rise in the percentage of frauds committed by senior management. In the UK this category increased from 18% of all frauds in 2016 to 50% in 2018. In our experience, these types of fraud can relate to a range of activities, including the manipulation of accounting records to influence results and deliberate overcharging of customers where contractual arrangements may be vague.

Interestingly for UK businesses with operations overseas, accounting fraud or misstatement of results was by far the more common overseas fraud, with 40% of businesses affected. This is also by far the most disruptive fraud in organisations' overseas locations.

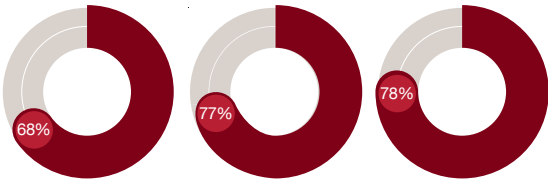
Many businesses do not consider the risk of fraud from the perspective that the business or one of its subsidiaries may be the perpetrator, yet it is these types of fraud that are typically the most damaging to brand, reputation and shareholder value. Frauds perpetrated by management present some unique challenges:

- They are often harder to spot, as management may be in a position to override controls;
- As a result, the direct loss from the fraud can be much greater;
- Related activity may set a culture and "tone from the top" that unethical behaviour is acceptable;
- Employees may be pressured to turn a blind eye; and
- The incentives and pressures can be complex, for example, to maintaining the continuity of the business rather than for direct personal gain.

The wider cost of fraud

While some of the losses from fraud can be quantified clearly, others are much harder to understand. For example, on top of the losses sustained as a direct result of a fraud, businesses also face the costs of investigation and remedial activities, as well as potentially significant disruption to wider business activities.

Of those respondents who had experienced a fraud in the last two years:



68% said that the fraud had an impact on their reputation and brand

77% said it had an impact on business relations

78% said it had an impact on employee morale

At the same time, UK organisations are spending more than ever on compliance. 54% of UK organisations have seen an increase in compliance spend over the past two years (vs 42% globally), and 51% expect it to increase in the next two years (compared to 44% globally). It is clear that UK businesses are taking compliance spending significantly more seriously than the global average.

Source: Global Economic Crime Survey 2018

Fraud risk assessments

Given the continuing rise in fraud, it is worrying that 50% of the UK businesses surveyed had not carried out a general fraud risk assessment, which looks at the key risks facing particular parts of their business or activities in the past two years. This is broadly consistent with the global position.

In our view, a well-considered and closely targeted assessment should be the technique that, first and foremost, drives all other anti-fraud activities. Its absence means that the business's other anti-fraud activities may be poorly targeted and lack effectiveness and specificity.

More positively, some companies do report undertaking more focused risk assessments relating to specific risk areas such as cyber vulnerability (52%), anti-bribery and corruption (50%), anti-money laundering (28%), sanctions and export controls (25%), and anti-competitive behaviour (17%). However, it's clear that coverage is patchy across all areas.

In our experience, very few organisations have put processes in place to identify major changes in the risk profile of the business or parts of the business, such as new products or new markets. Fraud risk assessments, when prepared, are often static documents, reflecting a snapshot at a moment in time, rather than responding to a complex and evolving environment. This type of static assessment is not enough.

Fraud risk is an increasingly multifaceted and complex issue that develops over time. Both fraud techniques and threats evolve alongside the business's activities, operations, people and structures.

This makes it vital that risk assessments are refreshed regularly to ensure developing threats are addressed, and means the lack of frequency with which we know risk assessments are being reviewed is a significant concern.

With risk assessments being an increasing feature of enforcement actions (as well as part of an "adequate procedures" or "reasonable procedures" defence under the UK Bribery Act and the Criminal Finances Act), it's more important than ever that a business's fraud risk assessment is fit for purpose. Key questions to consider include:

- Are you just focusing on the obvious areas, where you probably already have the best controls?
- When did you last update your risk assessment? Does it adequately reflect your business as it is today?
- Do you have a holistic view of fraud risks, or have your risk assessments been carried out in silos?
- Have you engaged with all relevant stakeholders, and do your senior management have a sufficient level of oversight?
- Would your risk assessment stand up to scrutiny in the event of an unexpected investigation under the Criminal Finances Act or the UK Bribery Act.

50%

of UK businesses surveyed had not carried out a general fraud risk assessment looking at key fraud risks in the past two years. This compares to 46% globally

Key questions to ask:

- Am I maintaining a view of my evolving risks – including fraud, cyber and bribery?
- Is this detailed and tailored to my organisation and how it operates?
- Are each of the risks identified covered by appropriate anti-fraud measures?

Technology 2.0:

How can you focus your resources and use technology more effectively?

49%

of the frauds in the past two years were cybercrime

The top fraud in the UK in 2018 was cybercrime, suffered by 49% of these respondents who had experienced fraud in the past two years. As a result it overtook the traditional "winner", asset misappropriation (32%), for the first time since our survey started. A closer look at the figures underlines the scale of the issue.

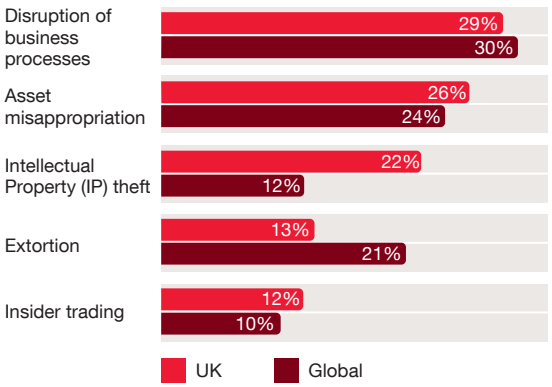
Given the number of high-profile cyber and data loss issues reported in the media recently, it isn't surprising that 42% of UK respondents felt that cybercrime will be the most disruptive economic crime over the next two years, far higher than the global average of 26%.

As a developed economy, the UK represents an attractive target, especially for overseas threat actors. Their attacks are causing significant business disruption, and are often used as a channel to commit more traditional frauds such as the theft of assets, cash, or Intellectual Property. Cybercrime is often simply a new take on old-fashioned confidence tricks, but can also be highly sophisticated.

As a result of its prevalence, impact and the requirements of EU General Data Protection Regulation (GDPR), cybercrime is high on the agenda for UK boards. One sign of this is that 82% of Chief Information Security Officers ("CISOs") in the UK report directly to the board, compared to only 61% globally. This echoes the findings from PwC's recent Global CEO Survey, which revealed that cybercrime was one of the top current concerns of business leaders.

Fortunately, UK business appears to be taking the challenge of cybercrime seriously, with a higher level of UK businesses than the global average having put cyber security programmes in place. That said, 25% of UK respondents still do not have such a programme, or are still evaluating whether to have one. This is a risky position to be in.

Exhibit 1: What type of economic crime was committed through cyber attack?



Source: Global Economic Crime Survey 2018

Gone Phishing?

Over half of the cyber attacks reported in the last year involved phishing, which seems to be more prevalent in the UK than in the rest of the world (20% higher than the global average). It could also be that the UK is just better at spotting phishing attacks.

However, what is clear is that phishing (a broader term to cover mass attacks that are playing the odds) or spear-phishing (more targeted attacks on an individual) are often just the starting point for a wider attack. Phishing allows fraudsters to gain access to a company's systems, whether for the purposes of stealing information, blackmail, or simply to cause disruption.

Email filtering will catch some phishing attacks, but given that businesses almost always need to let through external emails, it is difficult to catch every phishing attack.

Also, criminals' phishing tactics are changing over time. The consequences of attack can be devastating, so awareness and diligent behaviour on the part of technology users is a vital defence. Phishing capitalises on our vulnerabilities as humans, playing on our curiosity or fear and acting as a trigger that causes us to do something we wouldn't usually do. Phishing files are deliberately titled to exploit human behaviour – names such as 'Pay_details_for_all_staff.xls' and 'Planned_redundancies.ppt' have both been used in the past.

Ultimately, defence against phishing attacks relies on humans, as well as technology, so training, awareness and escalation procedures are key tools to use.

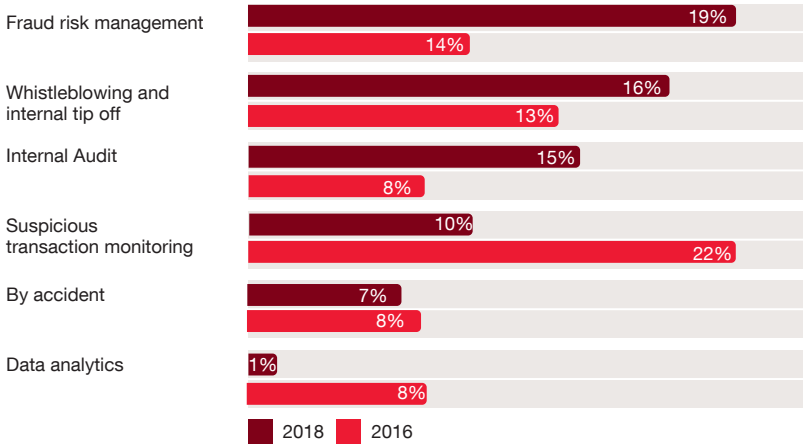
Technology and fraud detection

the most successful fraud detection methods in 2018 have relied on people

This year, our survey shows that the most successful fraud detection methods in the UK rely on people – with fraud risk management techniques (detecting 19% of frauds), internal tip offs and whistleblowing (detecting 16% of frauds) and internal audit (detecting 15% of frauds) coming out top. The percentage of frauds detected by all of these methods has increased compared to 2016, suggesting that anti-fraud measures are getting better at detecting issues.

However, while people-based detection methods are essential, they can also be labour and cost intensive. In the current climate, the best fraud detection harnesses the power of both people and technology to balance higher effectiveness, with tight control of costs.

Exhibit 2: How are companies detecting fraud?



Source: Global Economic Crime Survey 2018

Making technology work for you, not against you

When technology is used well, it can be of a real benefit to the business: 70% of respondents highlighted that technology tools enable them to carry out real-time monitoring, and 67% said it gave them insights that were actionable.

However, the benefits offered by technology are not being reflected in detection rates. The percentage of frauds detected by technology has decreased since our last survey, especially in the key areas of suspicious transaction monitoring and data analytics.

It is important to note that a wide range of activities can be termed data analytics, ranging from simple spreadsheet techniques to far more complex predictive techniques using specialist software. When it comes to using more advanced techniques such as predictive analytics (used by 15% of respondents in the UK compared to 18% globally), continuous monitoring (used by 41% of respondents in the UK compared to 49% globally) and machine learning (used by 14% of respondents in the UK compared to 18% globally), the UK seems to be lagging behind the rest of the world. Less than 10% of the UK respondents who are using technology are getting value out of these technologies, and a quarter have no plans to use artificial intelligence at all. So there is a clear need for more innovation in fraud prevention technology in the UK.

The known unknowns: what is lurking in your data?

With data analytics detecting only 1% of frauds in the UK (compared to a global average of 4%), it seems that many UK organisations are missing out on two key opportunities that analytics present: first, to detect anomalies within their data; and second, to get a better understanding of their business to help drive commercial decisions.

One area where good analytics can make a real difference is in tackling procurement fraud. We've seen a 28% rise in the number of organisations in the UK experiencing procurement fraud, and it's clear that this type of fraud represents a significant hidden cost, particularly in high-volume, lower-margin businesses. It often takes a long time for procurement fraud to come to light and, over the years, we have seen many examples where millions of pounds have been stolen.

However, these sorts of frauds do leave traces. Advanced analytics and visualisation tools can readily spot these traces, and detect unusual patterns of behaviour that are indicative of either fraud or a wider control or process weakness that should be addressed.

<1%

Data analytics detected only 1% of frauds in the UK (compared to a global average of 4%)

Key questions to ask:

- Am I taking steps to manage the risks posed by cyber threats and GDPR?
- Is my current anti-fraud data analysis fit for purpose?
- Am I investing in the right anti-fraud technology?
- Does my data analysis focus on specific fraud risks e.g. bribery?

Bribery 2018:
the ongoing impact of the UK Bribery Act on business' approach towards bribery and corruption

23%
the number of organisations experiencing bribery and corruption in the past two years has increased from 6% to 23%

One of the most surprising statistics in this year's survey was the big increase in the proportion of UK organisations that reported having experienced bribery and corruption in the last two years – a figure that has leapt to 23% from just 6% in 2016 (with the global average in 2018 being 25%).

While research done by observers such as Transparency International, indicates that the level of bribery and corruption in the UK remains relatively low from a global perspective, our survey suggests that the issue is having a serious impact on our UK respondents.

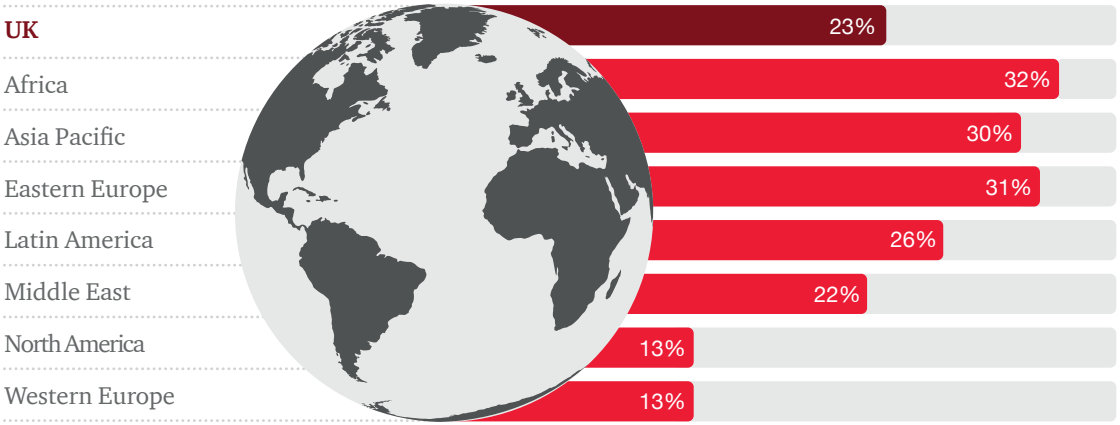
Our survey also finds that nearly a quarter of UK businesses had been asked to pay a bribe in the past two years, either in the UK or in their overseas operations. In 2016, only 5% reported that they had been asked to pay a bribe.

So, is this trend telling us that bribery is suddenly more prevalent in the UK? Or is something else going on? Our experience tells us that it's the latter.

Policies, backed up by actions

In the past ten years, the UK has gone from lagging behind the rest of the world in its anti-bribery laws and enforcement activities, to being at the forefront of global anti-corruption efforts. It now appears that these developments, and the greater openness they have helped to generate, are having a significant impact on our UK findings.

Exhibit 3: What percentage of those who experienced fraud experienced bribery & corruption?



Source: Global Economic Crime Survey 2018

The UK Bribery Act, which came into force in 2010 has been instrumental in bringing to light a number of high-profile cases, and has without doubt led to huge improvements in how UK business prevents and detects bribery. It has also led to massive increases in the sums business spends on ensuring compliance. At the same time, the UK has remained committed to an agenda of fostering transparency and responsible business behaviour, as set out in the recently published UK anti-corruption strategy 2017-2022. Both the OECD (Organisation for Economic Co-operation and Development) and Transparency International have praised the UK's efforts, particularly with regard to foreign bribery offences.

This commitment to tackling bribery is also evident among UK businesses. Three-quarters of the UK respondents to our survey said their organisation had a formal ethics and compliance programme in place. Of these, 62% said that this included specific anti-bribery and corruption policies, well above the global average of 50%. These figures indicate that a number of factors, including an increased focus on creating a culture of transparency, the promotion of whistleblowing hotlines, and encouragement from the authorities for organisations to self-report, have all contributed to an environment in which UK organisations are far better informed than only a few years ago regarding potential incidences of bribery and corruption in their global operations.

3/4

of the UK respondents to our survey said their organisation had a formal ethics and compliance programme in place

Managing your bribery and corruption risk

The starting point for developing processes and controls to manage bribery and corruption risk should be conducting a risk assessment – this is also the first principle of "adequate procedures" under the UK Bribery Act. Given this, and the number of cases of bribery and corruption that have been in the news recently, it is surprising that only half of respondents to our survey had carried out a bribery risk assessment in the past two years.

In addition, we found that a significant minority of respondents are not using any kind of monitoring technology in relation to bribery and corruption. While these kinds of frauds are, arguably, harder to detect than cyber breaches (which the vast majority of respondents do use technology to monitor), all organisations have access to data that, if analysed properly, will enable them to pinpoint anomalies and inconsistencies that require further investigation. This approach is particularly relevant in relation to bribery, as such ongoing monitoring is a key part of any "adequate procedures" defence, and is also an area where we see many organisations struggling.

The legacy of historical offences

Of those UK respondents who had experienced fraud in the past two years, only 5% felt that bribery and corruption had the most disruptive impact on their business. This may be because many have spent considerable sums putting in place extensive compliance activities and frameworks, and believe the risk of future bribery and corruption is low.

Significantly, a large proportion of the high-profile cases that have come to light recently have been historical in nature, involving investigations centred on allegations of improper behaviour stretching back many years. Many of these have been uncovered through the recent focus on corporate integrity.

Similarly, looking forward, only 10% of respondents think that bribery and corruption will be the most disruptive economic crime that they experience over the next two years.

The risks of doing business

Whilst there has been a sustained effort in the UK to tackle bribery and corruption, our survey suggests that this type of fraud is still having a big impact on UK organisations. As an illustration, some 21% of our UK respondents felt that they had lost an opportunity to a global competitor who they believed had paid a bribe, up from just 7% in 2016.

The UK's strong focus on the anti-bribery and corruption agenda may also explain why over half of our respondents reported that they included specific anti-bribery and corruption due diligence as a part of work undertaken when acquiring another business.

This is higher than the global average of 45%, and second to regulatory compliance as a priority for due diligence.

This aligns with our experience of client demands for such services as well as even greater focus on volume based integrity due diligence on businesses' third parties. Such measures are sensible, given that 55% of fraud threats come from sources external to the organisations, as referred above.

21%

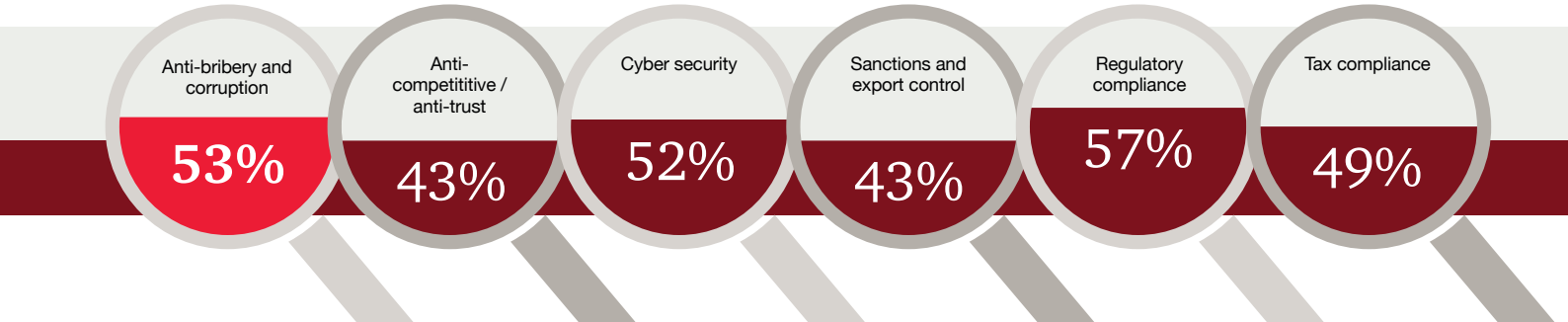
of the UK respondents felt that they had lost an opportunity to a global competitor who they believed had paid a bribe

Key questions to ask:

- Do I understand the detailed bribery risks facing my organisation?
- Is my programme of adequate procedures linked to these risks?
- Is the ethical due diligence on those I do business with adequate?

Exhibit 4: What additional due diligence do you do on acquisitions?

Source: Global Economic Crime Survey 2018



Contacts

If you want to know more about any of the issues discussed above, be it fraud or bribery risk, cyber threat prevention, forensic technology or integrity due diligence, then please contact one of our subject matter experts.

Fran Marwood
Investigations Partner,
Forensic Services
T: +44 (0) 20 7213 4709
M: +44 (0) 7841 491400
fran.marwood@pwc.com

Ian Elliott
Partner, UK Forensic
Services Leader
T: +44 (0) 20 7213 1640
M: +44 (0) 7711 912415
ian.elliott@pwc.com

Umang Paw
Head of Digital &
Forensic Investigations
M: +44 (0) 7931 304666
umang.paw@pwc.com

Mark Anderson
UK Anti-Bribery and
Sanctions Leader
T: +44 (0) 20 7804 2564
M: +44 (0) 7770 921256
mark.r.anderson@pwc.com

Survey editorial team
Kathryn Westmore
Senior Manager
T: +44 (0) 20 7213 2941
M: +44 (0) 7715 211090
kathryn.m.westmore@pwc.com

Marketing team
Jennifer Miranda
Marketing Manager
T: +44 (0) 20 7213 3939
M: +44 (0) 7715 033797
jennifer.miranda@pwc.com

www.pwc.co.uk/gecs

Design Services 31157 (02/18).