PwC's Global Economic Crime and Fraud Survey 2022

Protecting the perimeter:

The rise of external fraud

pwc

www.pwc.com/fraudsurvey

Environmental, geopolitical, financial and social pressures are creating a risk landscape that is more volatile than ever. This volatility complicates the challenge of preventing fraud and other economic crime. As organisations act quickly to navigate change, bad actors look to exploit the potentially widening cracks in fraud defences.

Are sufficient controls in place for the myriad new digital technologies being deployed? Are enterprises managing risks related to a sustained hybrid work environment? Have organisations implemented the appropriate policies and incentives as they emerge from the pandemic into an uncertain economy? What, exactly, is the fraud risk that companies face today?

Years of effort to combat fraud through policies, training, internal controls and monitoring have helped to tamp down internally driven misconduct, even in a volatile risk environment. Meanwhile, new, more impactful threats have been brewing. This year's Global Economic Crime and Fraud Survey shows that organisations' perimeters are vulnerable, and external fraudsters are emerging as a bigger threat.

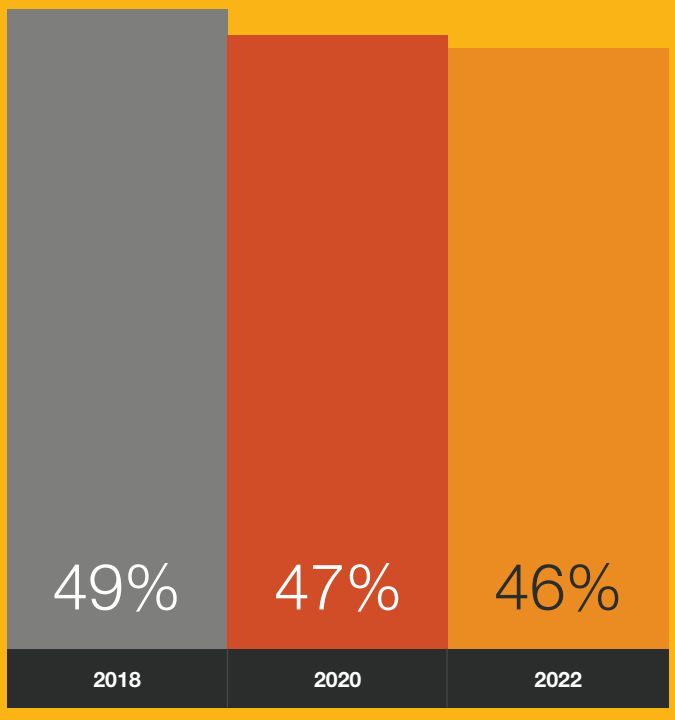
1

Fraud prevention measures are working

There's some good news in our survey. Overall, fraud, corruption and economic crime rates show no increase since 2018, despite supply chain issues, environmental and geopolitical instability, an uncertain economy, a talent shortage and many emerging risks. Just under half of organisations (46%) reported experiencing some form of fraud or other economic crime within the last 24 months.

The tech industry is a notable exception. The growing maturity of the sector helped it identify a significant increase in fraud activity since 2020. Nearly two-thirds of technology, media and telecommunications companies experienced some form of fraud, the highest incidence of all industries.

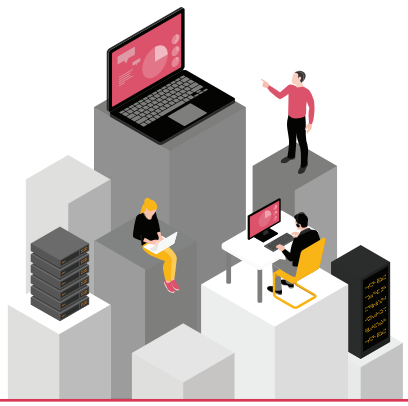
Share of organisations experiencing fraud, corruption or other types of economic crime



Source: PwC's Global Economic Crime and Fraud Survey 2022

Although rates of fraud and economic and financial crime are stable, the impacts of those crimes are substantial among both large and small organisations (as measured by annual revenues). Among companies with global annual revenues over US$10bn, 52% experienced fraud during the past 24 months; within that group, nearly one in five reported that their most disruptive incident had a financial impact of more than US$50m. The share of smaller companies (those with less than US$100m in revenues) affected was lower; 38% experienced fraud, of which about one in four faced a total impact of more than US$1m.

What are the greatest risks? Across organisations of all sizes, cybercrime poses the biggest threat, followed by customer fraud and asset misappropriation. (Our 2020 survey reached similar conclusions.)



46%

of surveyed organisations reported experiencing some form of fraud or other economic crime within the last 24 months.

Fraud rates and financial impact among large and small organisations

Companies with more than US$10bn in revenue

52%

experienced fraud in the last 24 months.

18%

of those companies had US$50m or more in financial impact from their most disruptive fraud incident.

Companies with less than US$100m in revenue

38%

experienced fraud in the last 24 months.

22%

of those companies had US$1m or more in financial impact from their collective fraud incidents.

Source: PwC's Global Economic Crime and Fraud Survey 2022

Organisations are doing the hard work of enhancing technical capabilities and implementing stronger internal controls.

Types of fraud experienced, by organisation size (in global revenue)

	Less than US$100m	US$100m–$1bn	US$1bn–$10bn	More than US$10bn
1	Cybercrime 32%	Cybercrime 41%	Cybercrime 42%	Customer fraud 35%
2	Customer fraud 27%	Customer fraud 32%	Customer fraud 34%	Cybercrime 32%
3	Asset misappropriation 23%	Asset misappropriation 23%	Asset misappropriation 24%	Asset misappropriation 31%

Source: PwC's Global Economic Crime and Fraud Survey 2022

The outlier to the dominance of cybercrime is the energy, utilities and resources (EU&R) sector, where procurement fraud is the biggest threat. Of the 31% of EU&R companies experiencing crimes, nearly half reported procurement fraud. With a smaller digital footprint and fewer customer interactions than many other sectors, it makes sense that this industry's fraud profile would be different than that of other sectors. Nonetheless, recent events have shown that cyberattacks against infrastructure could pose a looming threat in the near future.

Systematic changes are helping to bolster organisations against fraud and other economic crimes. Specifically, they have implemented policies, procedures and training to help employees who want to do the right thing. But the survey affirms that organisations are now doing the hard work of enhancing technical capabilities and implementing stronger internal controls and reporting measures. Two-thirds of organisations that experienced fraud discovered their most disruptive incident through corporate controls, up seven points from 2020.

Types of fraud experienced, by industry

Industrial manufacturing	Financial services	Energy, utilities and resources	Retail and consumer	Government and public sector	Health industries	Technology, media and telecommunications
Cybercrime	Customer fraud	Procurement fraud	Customer fraud	Cybercrime	Cybercrime	Cybercrime
32%	44%	45%	37%	36%	40%	50%
Asset misappropriation	Cybercrime	Cybercrime	Asset misappropriation	Asset misappropriation	Asset misappropriation	Customer fraud
28%	38%	29%	31%	33%	30%	35%
Accounting/ financial statement fraud	Know-your-customer failure	Supply chain fraud	Cybercrime	Customer fraud	Customer fraud	Procurement fraud
24%	29%	29%	27%	28%	27%	26%

Source: PwC's Global Economic Crime and Fraud Survey 2022

IN FOCUS

Fraud in a downturn

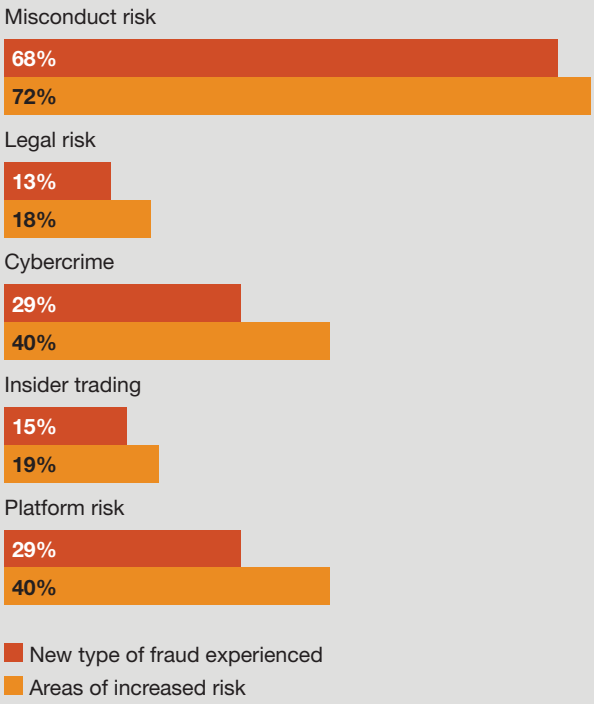
The pandemic created unsettling vulnerability as organisations accelerated the shift to digital operations. One bright spot is that asset misappropriation, while still a top category of fraud, was down in the last 24 months—perhaps, in part, because more employees are now working remotely, with limited access to company assets. At the same time, remote working increased risks beyond just digital security. For example, some companies experienced increased risks to employee safety; there was a heightened risk of blackmail or physical harm to employees working from home with access to valuable corporate data. The rate of organisations experiencing disinformation fraud in the past 24 months was 15%, suggesting companies need to increase their awareness of this emerging risk. (Listen to PwC's podcast on ways to fortify against disinformation.)

Past downturns, such as the 2007–09 recession, offer valuable lessons for organisations navigating volatility as they begin to emerge from the pandemic. History shows that fraud trends in a time of turmoil don't emerge immediately. Often, it takes 18 to 24 months for these events to become known. However, inflection points, such as the shift from a shrinking to an expanding economy, can be beacons for internal fraud identification.

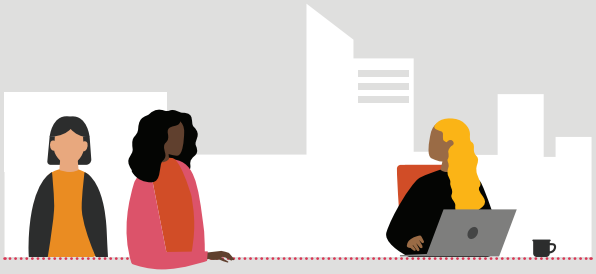
Much internal fraud can become visible in times of transition because fraudster behaviour lags the shift to new goals and targets. For example, corrupt employees may be taking illegal actions to achieve sales targets that leaders know are unobtainable heading into a down economy, and therefore suspicious. External fraudsters also capitalise on inflection points, taking advantage of the market confusion, particularly with consumer-based schemes. Organised crime groups can recruit more easily in a down economy, bringing in new team members who are suddenly unemployed. As a result, there's every reason to increase scrutiny on fraud risks in a downturn, with special attention to those the organisation may not have seen before.

Economic crime due to COVID-19

Share of companies that say they experienced new fraud and increased risk because of COVID-19



Source: PwC's Global Economic Crime and Fraud Survey 2022



70%

of those encountering fraud experienced **new incidents** of fraud as a result of disruption caused by COVID-19.

2

The perimeter is vulnerable, and the game has changed

The survey identifies an unsettling threat profile emerging. Dangerous new predators—external entities that can't be controlled or easily influenced—are quickly growing in strength and effectiveness. Nearly 70% of organisations experiencing fraud reported that the most disruptive incident came via an external attack or collusion between external and internal sources. And external fraudsters are immune to traditional fraud prevention tools such as codes of conduct, training and investigations.

The impact of hackers and organised crime rings, which are among the most common external perpetrators, rose substantially in the last two years. About one-third of external perpetrator cases were the result of hackers, and 28% were conducted by organised crime; both numbers reflect increases from our 2020 survey.

Main perpetrator of the most disruptive or serious fraud experienced

External perpetrator

43%

(41% in 2020)

Organisations in Europe are significantly more likely than those in other regions to experience fraud perpetrated by external actors (56%).

Internal perpetrator

31%

(38% in 2020)

Where an organisation's most disruptive fraud derived from misconduct risks, it was significantly more likely to be caused by internal perpetrators in comparison to cyber risks (35% vs.16%).

Collusion between internal and external actors

26%

(21% in 2020)

Organisations in China/Hong Kong were significantly more likely than those in other regions to experience fraud perpetrated by collusion between internal and external actors (50%).

Source: PwC's Global Economic Crime and Fraud Survey 2022

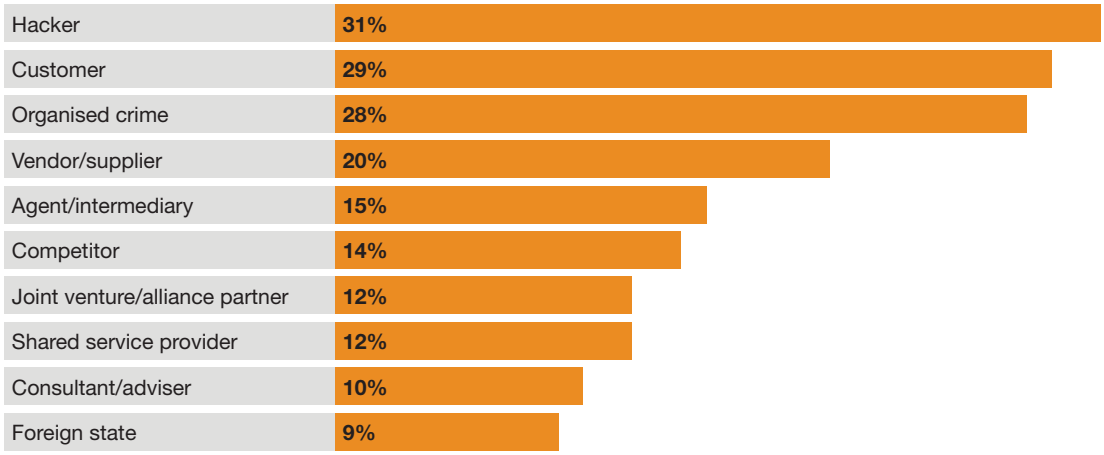
Organised crime groups are becoming more specialised and professional, with goals, incentives and bonus structures. They take advantage of vulnerabilities, and they invest continuously to outsmart their prey. Combatting these bad actors is unlike the effort to contain internal fraud, because companies have little ability to influence or control the perpetrators' actions.

Several factors are converging to drive a rise in external fraud. The increased frequency of data breaches in recent years will undoubtedly continue, raising the bar considerably for companies obligated to protect the private, personally identifiable information of their customers. The breaches will also challenge the knowledge-based authentication strategies that organisations have put in place to protect against fraudsters.

Bad actors are also collaborating, which increases both the volume and sophistication of attacks. Thanks to chat rooms, the dark web and cryptocurrency, specialists in data breach, false ID creation, attack methodology and other nuanced areas can connect, coordinate and transact within a growing criminal economy. (Listen to PwC's podcast on the rise of ransomware attacks.)

In addition, there's a rising trend of formerly law-abiding people joining fraudster groups. The trend is particularly prevalent in nations with poor socioeconomic conditions, enabling people to rationalise such actions because they have fewer legitimate economic opportunities.

Type of external perpetrator



Top external perpetrators, 2020

1 Customer 26%

2 Hacker 24%

3 Vendor/supplier 19%

Source: PwC's Global Economic Crime and Fraud Survey 2022

3

Platforms are the new fraud frontier

Of those organisations experiencing fraud in the last two years, four in ten experienced some form of fraud connected to the digital platforms they rely on, whether that was related to know-your-customer (KYC) breaches, disinformation, money laundering, terrorism financing or anti-embargo activities. The rise of digital platforms, such as social media, e-commerce or services (for example, rideshare or lodging) opens the door to myriad fraud and other economic crime risks that most companies are just beginning to appreciate.

Platform risks can create a ripple effect—with the impact of fraud penetrating multiple organisational silos. Because platform fraud is an enterprise-wide problem, combatting it requires an organisation-wide, cross-functional effort with a diverse community of solvers.

Understand your platform risks by taking our survey, and watch for deeper insights on platform fraud coming soon.

IN FOCUS

Emerging threats

Emerging risks have the potential to cause greater disruption in the next few years. By definition, these risks are low on the radar. But they can move to the forefront quickly. For example, just 6% of organisations said they experienced anti-embargo fraud in the last 24 months. But that is likely to change in the next 24 months as global sanctions rise to the highest levels in recent history.

The challenge with managing emerging fraud risks is to avoid falling into the trap of only seeing what is known and not seeing what is unknown. What are those emerging fraud risks of potentially greatest concern? PwC believes at least two should be on the radar.

ESG reporting fraud. Trust has become a key lever for value creation. PwC's 25th Annual Global CEO Survey highlighted the relationship between companies with a high level of trust and their ability to drive change. But trust is fragile. A perceived or real misstep in transparency can wreak havoc on brand reputation and underlying trust. With environmental, social and governance (ESG) responsibility growing in importance to stakeholders, accuracy in ESG reporting is essential. Just 8% of those organisations encountering fraud in the last 24 months experienced ESG reporting fraud, but the incentive to commit fraud in this area is only going to increase—as will the consequences.

Supply chain fraud. One in eight organisations experienced new incidents of supply chain fraud as a result of the disruption caused by COVID-19. One in five sees supply chain fraud as an area of increased risk as a result of the pandemic. Few companies are aware of the fraud and misconduct risks within their supply chain, making this an area of exposure now and into the future.

6%

of organisations said they experienced **anti-embargo fraud** in the last 24 months.

8%

of those organisations encountering fraud in the last 24 months experienced **ESG reporting fraud.**

1 in 8

organisations experienced new incidents of **supply chain fraud** as a result of the disruption caused by COVID-19.

Key considerations for protecting your perimeter

Respondents to the survey indicate they are strengthening internal controls, technical capabilities and reporting to prevent and detect fraud. However, defending against external predators requires a different set of tools. With external fraud growing, here are three considerations to help shore up your perimeter.

1. **Understand the end-to-end life cycle of customer-facing products.** Take the time to identify where opportunities exist for a fraudster to exploit a product and cause financial, legal or reputational damage. How could it happen, what would it take to prevent it from happening, and what type of response is needed if it happens?

2. **Strike the proper balance between user experience and fraud controls.** Protecting customer-facing channels will require a delicate balance between ensuring that users have a great experience and detecting and stopping fraudsters. The dual objectives of keeping false positives as low as possible and catching true fraud can be achieved through a combination of fraud technology, strategy and processes.

3. **Orchestrate data.** Often, fraud signals will come from disparate, disconnected systems and are only detectable through the occasional manual review. It is crucial that fraud indicators are orchestrated into a centralised platform that can track the end-to-end life cycle of users (fraudsters or not) and generate meaningful alerts.

Conclusion

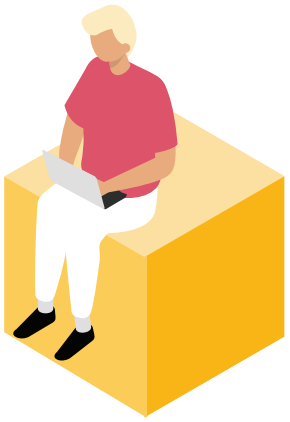
Preventing fraud and other economic crimes is a complex challenge. It takes a continuous focus on policies, training and internal controls and—increasingly—the use of sophisticated technology. In this volatile environment, protecting the perimeter is essential, as all signs point to formidable bad actors becoming better and better at exploiting the cracks.

About the survey

This year's Global Economic Crime and Fraud Survey enquired about organisations' attitudes towards fraud and financial and economic crime in the current environment and drew responses from 1,296 respondents in 53 countries and regions. This survey, our first snapshot of 2022, homed in on fraud trends and conduct risk.

For more than 20 years, PwC's Global Economic Crime and Fraud Survey has looked at a number of crimes, including:

- Accounting/financial statement fraud
- Anti-competition/antitrust law infringement
- Asset misappropriation
- Bribery and corruption
- Customer fraud
- Cybercrime
- Deceptive business practices
- Human resources fraud
- Insider/unauthorised trading
- Intellectual property (IP) theft
- Money laundering and sanctions
- Procurement fraud
- Tax fraud



61%

of survey respondents sit in the C-suite.

39%

of respondents' organisations have annual revenues greater than US$1bn (and 65% have revenues of more than US$100m).

Contacts

Kristin Rivera
Global Forensics Leader, Partner, PwC US
kristin.d.rivera@pwc.com

Ryan Murphy
US Forensics & Investigations Leader, Partner, PwC US
ryan.d.murphy@pwc.com

Claire Reid
UK Forensics Services Leader, Partner, PwC UK
claire.reid@pwc.com

Claudia Nestler
Germany Forensics Services Leader, Partner, PwC Germany
claudia.nestler@pwc.com

Mark Rigby
Australia Forensics Services Leader, Partner, PwC Australia
mark.rigby@pwc.com

Sirshar Qureshi
EMEA Forensics Co-Leader, Partner, PwC Czech Republic
sirshar.qureshi@pwc.com

Stefan Heißner
EMEA Forensics Co-Leader, Partner, PwC Germany
stefan.heissner@pwc.com

www.pwc.com/fraudsurvey