



**PwC's Global Economic Crime and
Fraud Survey 2022: India Insights**

Protecting the perimeter:

**Uncertainties and
the rise of external fraud**





Organisations across the world are facing a new risk landscape that has emerged due to environmental, geopolitical, financial and social pressures. Indian organisations are equally at risk in this extremely volatile new world that is complicating the challenges of preventing fraud and economic crime.

Table of contents

- 1** About the survey
- 2** Fraud prevention measures are working
- 3** The perimeter is vulnerable, and the game has changed: Rise in external fraud post COVID
- 4** Greater prevalence of fraud amongst big firms
- 5** Surge in customer fraud
- 6** Misconduct and platform risks on the rise
- 7** Emerging threats

1



About the survey

PwC's Global Economic Crime and Fraud Survey (GECS) 2022¹ surveyed 1,296 organisations across the world, out of which 112 were from India and represented 32 diverse industries. An overwhelming 76% of the respondents from India sit in the C-suite. The India survey covered both small and large organisations.

GECS 2022 surveyed

112 companies in India from 32 diverse

industries such as technology, media and communications, financial services, health services, consumer products and retail, industrial manufacturing and energy, utility and resources.



76%

respondents sit in the C-suite.

1 | <https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html>

2



Fraud prevention measures are working

Companies in India have been undertaking measures to combat fraud for several years now. The good news is that fraud prevention measures are working — 52% of Indian organisations experienced fraud or economic crime within the last 24 months, as opposed to 69% in our 2020 survey.

52%

of Indian organisations experienced fraud or economic crime within the last 24 months.



Financial impact on Indian organisations

40%

of these companies lost between USD 50,000–100,000

17%

lost between USD 1 million–50 million

5%

incurred a loss of USD 50 million and above through the most disruptive incidents of fraud/crime

3



The perimeter is vulnerable, and the game has changed: Rise in external fraud post COVID

Following the outbreak of the COVID-19 pandemic, organisations faced a huge amount of uncertainty, and a majority of them shifted to digital operations in order to minimise disruption. With employees working from home, companies were exposed to new risks related to digital security, employee safety and disinformation, and this in turn led to new incidents of fraud. An overwhelming 95% of companies that encountered fraud in India experienced new types of fraud as a result of the disruption caused by COVID-19.



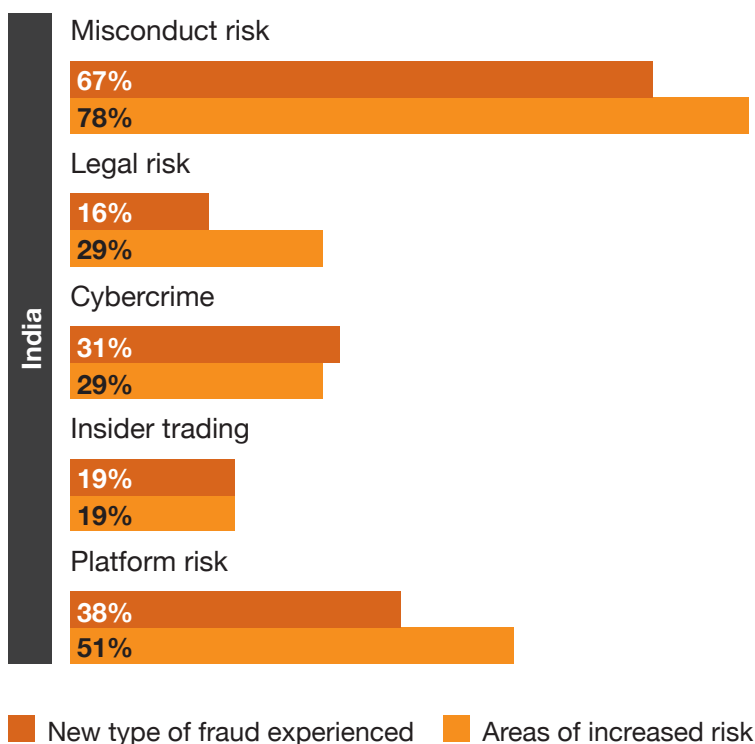
95%

of companies that encountered fraud in India experienced new incidents of fraud as a result of disruption caused by COVID-19.



Frauds and economic crimes due to COVID-19

Share of companies in India that said they experienced new incidents of fraud and increased risk because of COVID-19



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

Main perpetrator of the most disruptive or serious fraud experienced



External perpetrator

43%



Internal perpetrator

33%



Collusion between internal and external actors

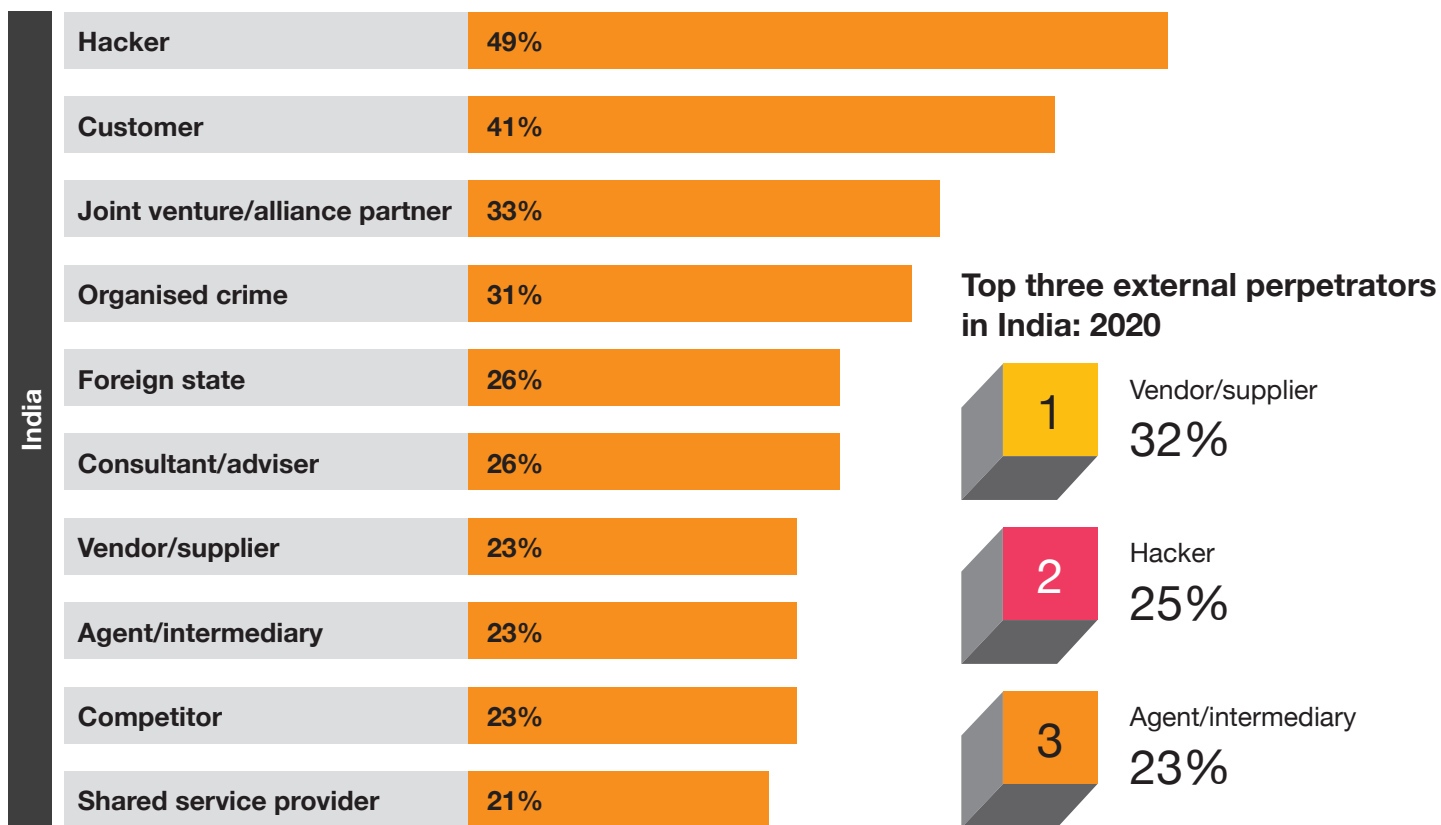
24%

The pandemic has made organisational perimeters more vulnerable and external fraudsters are emerging as a major threat. These external entities are more difficult to control or influence. Nearly 67% of organisations in India that experienced fraud reported that the most disruptive incident came via an external attack or collusion between external and internal sources. This proportion was 56% in our 2020 survey.

External fraudsters are immune to traditional fraud prevention tools, such as codes of conduct, training and investigation. Among the external perpetrators of fraud, 49% were hackers, 41% were customers and about 31% involved organised crime.



The perimeter is vulnerable: Types of external perpetrators

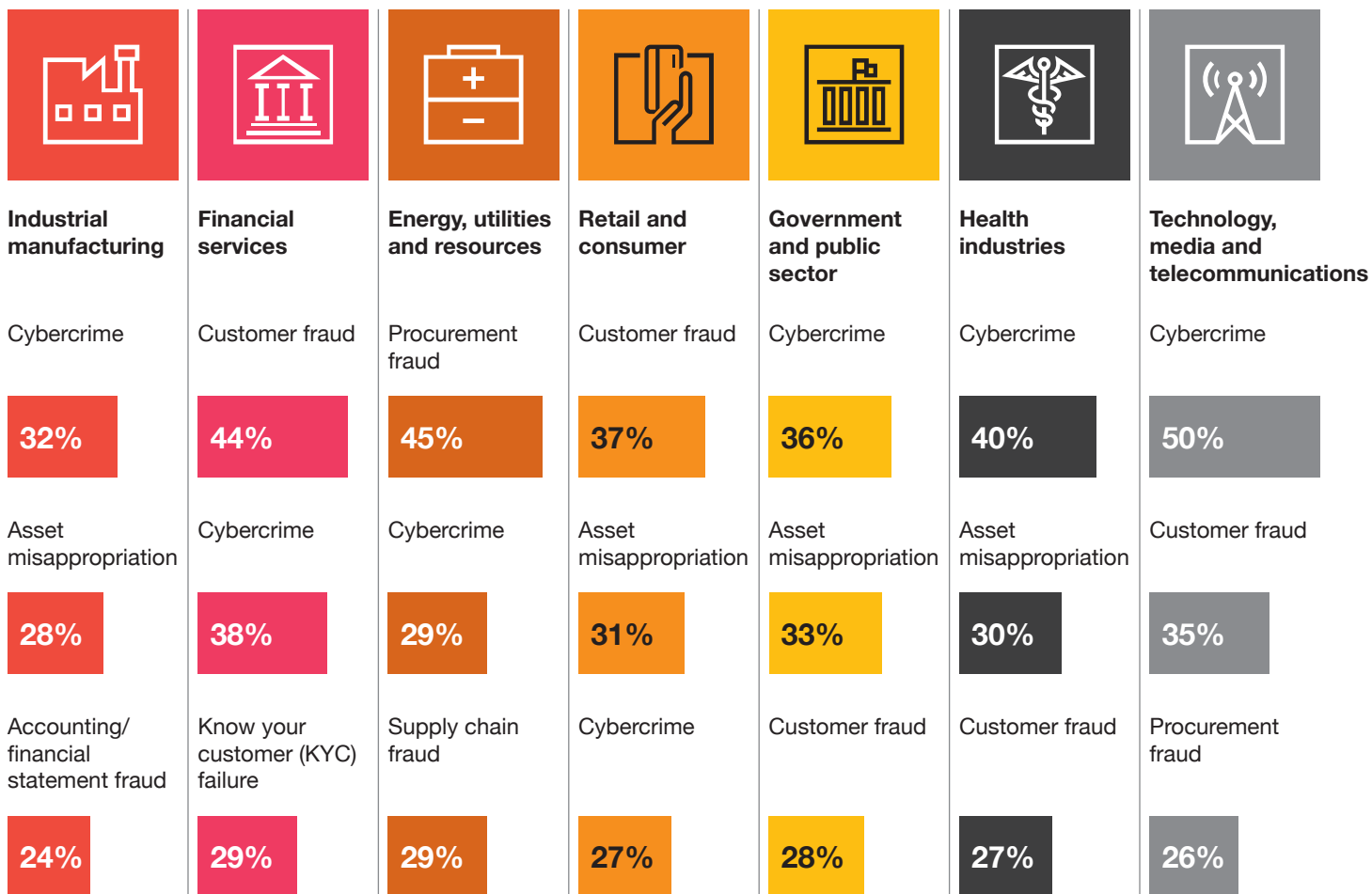


Source: PwC's Global Economic Crime and Fraud Survey 2022





Types of fraud experienced globally, by industry



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



4



Greater prevalence of fraud amongst big firms

Fraud and economic crimes impact both big and small firms. However, the survey found fraud to be more prevalent amongst big firms: 60% of companies surveyed in India having global annual revenues above USD 1 billion experienced fraud during the past 24 months (globally, 52% of organisations with revenues over USD 10 billion experienced fraud). The impact on smaller companies was less extensive as only 37% of companies in India with global annual revenues below USD 100 million experienced fraud during the past 24 months (global: 38%).

In terms of financial loss, 14% of firms surveyed lost USD 50 million or more, 28% lost between USD 1–50 million, and 50% of firms surveyed lost less than USD 1 million due to all incidents of fraud, corruption or other economic/financial crime over the last 24 months.

60%

of companies with global annual revenues of USD 1 billion or more experienced fraud over the last 24 months.



5



Surge in customer fraud

Our 2020 survey had found cybercrime, accounting/financial statement fraud, and bribery and corruption to be the top three frauds in India. Though globally, the findings of this year's survey are similar to those of GECS 2020, for India, the top frauds have changed significantly. In India, customer fraud (e.g. frauds involving mortgage, credit cards, claims, cheques)

was the top fraud reported by 47% of companies. Cybercrime came a close second, with 45% of Indian organisations reporting this type of fraud. Further, KYC failure was experienced by 34% of Indian firms that experienced fraud, corruption or economic/financial crime in the last 24 months.

Top five frauds faced by Indian organisations

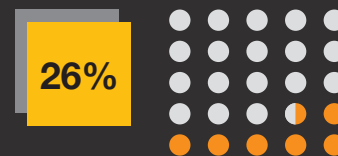
Customer fraud



KYC failure



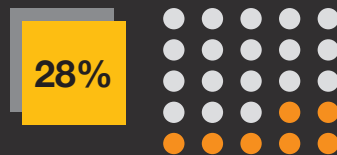
Procurement fraud



Cybercrime



Tax fraud



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

6



Misconduct and platform risks on the rise

The pandemic saw a rise in new impactful threats. Misconduct was the biggest challenge faced by organisations as bad actors began collaborating and taking advantage of pandemic-related uncertainty and volatility. Amongst organisations that reported fraud, conduct risk (or risks associated with individuals within the firm, or vendors, agents and customers) was the biggest threat at 90%.



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

Top four most disruptive frauds

Frauds that had the most disruptive or serious impact on Indian organisations (monetarily and otherwise):

1. **Cybercrime:** Unauthorised access to, or use of, an organisation's information systems and/or data (26%)
2. **KYC failure:** Inadequate controls or measures to verify customer information, resulting in fake or fraudulent activities (12%)
3. **Customer fraud:** Fraud perpetrated against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others (10%)
4. **Accounting/financial statement fraud:** Alteration or presentation of financial statements and/or other documents in a way that does not reflect the true value (9%)



With the rise of digital platforms to perform business operations, platforms have emerged as new fraud frontiers. Platform risks, or risks associated with digital platforms such as social media, services (rideshare, lodging) and e-commerce, have increased substantially. They were reported by 53% of organisations surveyed in India.

Cybercrime had the most serious impact on Indian organisations — with 45% of companies that faced fraud over the last 24 months (global: 37%) having encountered a cyberattack. Insider trading was also a big contributor, with 33% of companies that experienced fraud reporting it. At 24%, legal risks were also a significant challenge.

Categories of fraud faced by Indian organisations



90%
Conduct risk



53%
Platform risk



45%
Cyber



33%
Insider trading



24%
Legal risk

Different kinds of crimes, lapses and frauds under these categories

- 52% | Customer fraud
- 29% | Procurement fraud
- 25% | Accounting/financial statement fraud
- 23% | Bribery and corruption

- 65% | KYC failure
- 32% | Disinformation/misinformation
- 26% | Money laundering and terrorism financing
- 16% | Anti-embargo

- 63% | Deceptive business practices (such as incentive abuse)
- 47% | Insider/unauthorised trading

- 79% | Anti-competition/law infringement
- 57% | Intellectual property (IP) theft

India

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



7

In focus

Emerging threats

Indian organisations are facing multiple emerging risks that have the potential to cause greater disruption in the coming years. One such area is **ESG reporting fraud** (the act of altering ESG disclosures so that they do not truly reflect the activities or progress of an organisation) — 12% of organisations experienced ESG reporting fraud.

Companies in India are facing several challenges in managing risks associated with ESG targets and reporting requirements, such as a general lack of understanding about ESG (reported by 45% of organisations surveyed), lack of ownership over ESG in the organisation (at 42%) and inability to accurately monitor or report ESG metrics within the organisation (46%). As ESG continues to increase in importance for stakeholders, the incentive to commit fraud in this area is likely to grow.

Another emerging area of disruption is **anti-embargo fraud** (participation in unsanctioned foreign boycotts, or when an organisation is tricked into breaking an embargo). Though just 9% of organisations experienced anti-embargo fraud over the last 24 months, this may change in the next two years as global sanctions rise to the highest levels in recent history.

Supply chain fraud also has the potential to cause greater disruption in the coming years — 19% of organisations experienced it in the last 24 months.

12%

of those organisations that encountered fraud in the last 24 months experienced ESG reporting fraud.



9%

of those organisations that encountered fraud in the last 24 months experienced anti-embargo fraud.



19%

of those organisations that encountered fraud in the last 24 months experienced supply chain fraud.





In focus

Emerging threats

Organisations also experienced increased risk due to **customer fraud** (30%) and **KYC failure** (22%) as a result of disruption caused by COVID-19. Globally, these percentages were much lower — 17% for customer fraud and 10% for KYC failure. With an increase in digital banking and payments, KYC fraud is another emerging risk that organisations need to watch out for.

Given the low level of digital literacy in India, KYC and customer frauds can prove to be a far greater risk for organisations in the future.





Key considerations for protecting your perimeter

Respondents to the survey indicate that organisations 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 PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

© 2022 PwC. All rights reserved.

Contact us



Puneet Garkhel

Partner and Leader, Forensic Services

puneet.garkhel@pwc.com

pwc.in

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2022 PricewaterhouseCoopers Private Limited. All rights reserved.

AW/November 2022 - M&C 20275