

KROLL



Confederation of Indian Industry

CII-Kroll India Fraud Survey

SECOND EDITION

October 2021



Inside

Foreword.....	03
Summary of Findings.....	04
The Who, How and Where of Risk.....	06
The Fraud Landscape in India: Fraudsters Go Online.....	10
• A Changing Modus Operandi	
• Failing Oversight	
How Organizations are Tackling Fraud.....	13
• Screening Staff	
• What Happens to Fraudsters?	
Looking Forward.....	17
• The Role of Government	
• Vigilance is Key	
Survey Methodology.....	20
References.....	20
About CII.....	21
About Kroll.....	21

Foreword

“The ultimate measure of a man is not where he stands in the moments of comfort, but where he stands at times of challenge and controversy.”

Martin Luther King Jr.

The risk of fraud is ever-present for businesses around the world. And its prevalence does not appear to vary much over time. In survey after survey, irrespective of company size or location, roughly between three quarters and four fifths of executives admit to having experienced fraud. Do Indian businesses suffer from similar levels of persistence?

We set out to benchmark the market with an *CII-Kroll India Fraud Survey* published first in June 2019 and found Indian businesses had a seemingly lower rate of fraud than elsewhere. However, this piece of apparent good news cannot be taken at face value. Since fraudsters naturally try to hide their tracks, low rates of admission of fraud might just mean that crimes are going undetected. Alternatively, given the stigma attached to having suffered fraud, it could equally mean executives were hesitant to reveal real numbers.

This second edition of the *CII-Kroll India Fraud Survey* was an opportunity to validate the findings of the first report and at the same time see how Indian companies have adapted (or not) to the evolving fraud landscape. However, it is not just fraud that has changed over the last two years. Any socioeconomic study carried out after the start of 2020 will necessarily be affected by the impact of the coronavirus pandemic.

Globally, the impact of COVID 19 has been significant, with major effects not only on the healthcare system but also on the economy. COVID-19's effects on the economy alone would be expected to coincide with an uptick in fraud, which has been found to correlate with economic freedom, poverty and GDP.¹ At the same time, though, the coronavirus pandemic has had several impacts on business operations that are relevant to fraud. India is no exception.

On one hand, it has potentially increased the board-level awareness of and vigilance to risks: faced with the COVID-19 threat, many management teams will have reviewed and revised corporate processes and operational safeguards. On the other, lockdowns and remote working have also forced management to devolve certain powers, potentially fostering spheres of influence that are relatively free from oversight.

These spheres are fertile ground for various types of fraud, such as the non-competitive appointment of favored suppliers or the creation of fictitious processes and approval mechanisms to siphon off funds or steal intellectual property.

The *CII-Kroll India Fraud Survey* also reflects an increase in corporate fraud amidst the pandemic with 65% of the companies suggesting they have been a victim of fraud. Beyond the traditional risks, cyber threats have further complicated the risk landscape. Perhaps reflecting increased exposure as workers move beyond the firewall, as per the survey, leaders feel their organizations will be more vulnerable to cyber challenges than to any other form of fraud in the future.

Against this backdrop, the results of the second *India Fraud Survey* should make for interesting reading. This is not a report about COVID-19, but the results are clearly conditioned by the pandemic. It illustrates the evolution of fraud under exceptional circumstances and will hopefully serve to remind Indian business leaders of the need for continued vigilance.


Aside from the unique events of the last two years, it will be key for the Indian business community to address fraud as circumstances return to normal. As COVID-19 fades from view, business leaders should turn their attention to this issue and ensure rates go down.

Summary of Findings


This section draws a comparative analysis based on findings from our fraud survey commissioned in 2019 and in 2021.

CORPORATE FRAUD IS ON THE RISE WITH INCREASED THIRD-PARTY RISKS AND COLLUSION

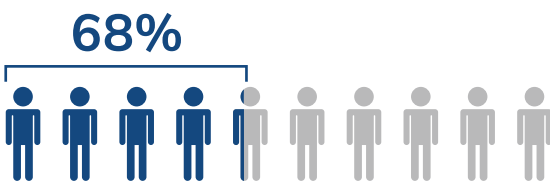


 Two in three companies experienced at least one fraud event as compared to 57% previously.



 Fraud triggered by conflicts of interest went from 10% to 26% and supply chain frauds increased to 14% from 5%

AND EXECUTIVES ARE TAKING A HARDER LINE AGAINST FRAUDSTERS



In 2019, only 44% of respondents said they would terminate a fraudster's employment, ask them to resign or suspend them. That number has now shot up to 68%.

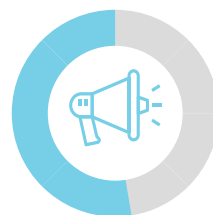


And 25% said they would report the employee to law enforcement, up from 15% in 2019.

BUT FRAUDSTERS ARE GOING DIGITAL AND ARE CAUSING REPUTATIONAL DAMAGE



Cyber threats are now one of the largest sources of fraud in India, affecting around a quarter of all businesses in the last 12 months.



Reputational damage remains the biggest threat from fraud, and it has risen in importance, being cited by 57% of respondents compared to 26% in 2019.

HELPED BY WEAK INTERNAL CONTROLS AND SLUGGISH DETECTION RATES



45% Weak controls were cited by 45% of respondents as a trigger for fraud.

But despite the rise of remote working, this is less of a factor now than it was in our last study, where 58% of respondents said weak controls contributed to fraud.

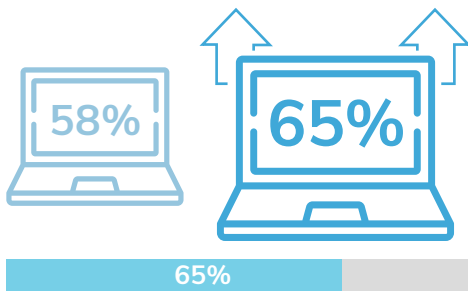
1/5 COMPANIES



Almost one in five companies took longer than three months to detect fraud and 12% said it had taken over a year.

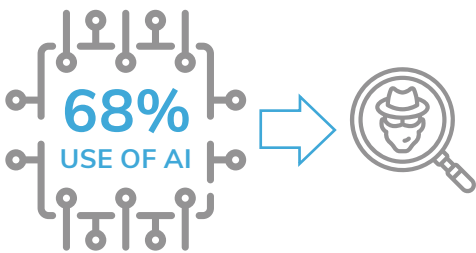
> 3 MONTHS/ 1 YEAR

HENCE, COMPANIES ARE STRENGTHENING GOVERNANCE AND IT SECURITY



Respondents reported an increase in all forms of anti-fraud measures, with IT security and certain governance measures being a particular highlight. **The proportion of companies strengthening IT defenses is up from 58% in 2019 to 65% in 2021.**

TECHNOLOGY IS THE PREFERRED GOVERNMENT TOOL FOR DEALING WITH FRAUD



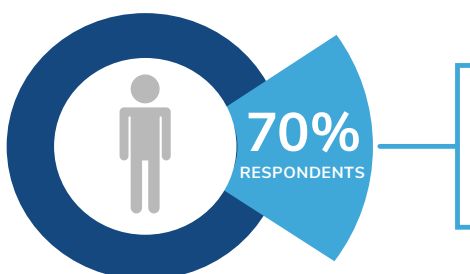
Respondents believe the Indian Government should use centralized reporting and faster court proceedings to help fight fraud. **But the most popular option, cited by 68%, was to use technology or AI for fraud detection.**

BUT CYBER FRAUD IS STILL THE BIGGEST THREAT GOING FORWARD



Reflecting its growing importance in the threat landscape, **executives ranked cyber fraud above all other risks** that organizations will be vulnerable to in the future.

AND BUSINESSES EXPECT FRAUD TO INCREASE



A worrying 70% of respondents believe fraud levels will grow in the coming year.

The Who, How and Where of Risk

It has been an unprecedented year for corporate risk, with firms simultaneously facing threats from all angles while managing the impact of COVID-19. Mitigating business risk has always relied on knowledge of markets and counterparties and the forces that could disrupt a company's agreements and assumptions. The broadening of the risk landscape is visible in the types of significant incidents the respondents of the *CII-Kroll Fraud Survey 2021* have experienced in the last 12 months and in the priority levels they assign to various risk mitigations.

Risk management today is centered on responding to—and trying to stay ahead of—rising threats while continuing to battle long-established risks. Newer risks differ from old ones in their ubiquity. While money laundering and counterfeiting, for example, take the greatest toll on particular industries and countries, virtually every enterprise is potentially vulnerable to social media attacks or collateral damage from a business partner's scandal. Adding urgency to the new risks is the need to establish appropriate systems and capabilities for combating them.

Worldwide, fraud-related incidents continue to take a heavy toll on organizations. Kroll's latest global research² suggests that the largest organizations felt the effects of this illicit activity most significantly, and there appears to be an inflection point, with firms with a turnover of \$10 billion-\$15 billion (48%) or above \$15 billion (57%) more likely to state the impact is very significant. This may be due to more complex company structures and supply chains, which in turn makes it harder to maintain visibility.

Board-Level Engagement

Internal business cultures that stress transparency and accountability as best practices are more effective at reducing the risk of frauds. Senior leaders play a crucial role in embedding this philosophy throughout an organization, establishing the proper tone from the top, aligning performance goals with ethical behavior and providing ongoing education to help employees navigate ambiguous situations.

It's a positive sign then that Kroll's global research² shows a growing focus on bribery and corruption in the boardroom, with 72% of respondents believing this challenge is being given sufficient board-level attention and investment. This is also a consistent opinion across different sectors, with the only notable outlier being the banking industry (53%), potentially since their focus is on preventing other illicit activities such as money laundering and sanctions breaches.

It appears that while board members are giving greater attention to certain risks, there is still a great divide between head office expectations and the local business practices in regional offices or supply chains. To bridge this divide and mitigate the fraud risk, organizations must go beyond blanket compliance policies. A top-down focus on long-term cultural messaging will be needed alongside nuanced data analytics, considering local business practices and attitudes.

Enterprise-Wide Risk Assessments and Internal Control Frameworks

Kroll's internal research² suggests that the vast majority (82%) of organizations have conducted an enterprise-wide risk assessment in the past five years to understand threats throughout their business. The global uptake of enterprise-wide risk assessments is surprisingly high, and though a positive, does not mean that the task is complete for businesses who have conducted one in the last five years. Very few organizations have updated their risk assessments to account for the changing post-COVID-19 landscape, so a risk assessment completed three years ago will no longer be sufficient.

Globally, we have witnessed that companies have grown in confidence in the ability of their internal control frameworks to detect and prevent high-risk activities when it comes to frauds. On average, three in every four companies believe their internal control framework is effective. This remains true for companies of all sizes and across different industries, although the least confident respondents were again from the banking sector (60%). The point to note, however, is that confidence in a control framework can only come from continuous testing—how can an organization know there is no problem until it looks? Also, an organization can have the best possible compliance program in place on paper, but if the human elements of the chain are not well-managed, educated or equipped to act, non-compliance or illicit behavior will continue to prevail and go undetected.

Organizations must undertake regular risk assessments and third-party audits and combine internal and external data for proactive analysis to identify risks early. Effective frameworks must also account for jurisdictional anomalies and cultural nuances to ensure the control environment is adapted to changing circumstances. Such careful compliance testing is not only crucial given the rising dependence on complex international supply chains but also now a legal requirement under many international anti-bribery laws.



Data Analytics

Kroll's global research² revealed that an unexpectedly high number (86%) of organizations are now using data analytics to detect fraud risk proactively. While it's encouraging that more businesses are leveraging these tools to their advantage, there are still doubts as to whether that advantage is being pressed hard enough. Live, data-driven monitoring that touches every tendril of a company's reach is what is needed, from field operatives to regional offices, and the technological potential is there. The question is, are businesses able to combine this technology with the human element of their business in a balanced and effective way?

Managing Third-Party Risk

Given the challenges organizations are facing with third-party risk, we can infer that most are not exploiting the full potential of data gathering and analytics as part of their ongoing third-party due diligence to provide adequate assurance over these elements.

To take control of both internal and external risks, companies must consider creative ways to receive reliable and timely on-the-ground information in all the places they do business. Organizations should then deploy a sophisticated approach to analyzing this information, running bespoke algorithms to spot anomalies not only at their headquarters and satellite offices, but also in their global supply chains. This "real-time monitoring" raises red flags that deserve further analysis to reveal either false positives or genuine issues. Furthermore, organizations need the ability to carefully calibrate their analytics based on a deep understanding of their business and corresponding risk profile, and the expertise to interrogate and verify results correctly. Only with such a sophisticated approach can organizations bridge the great divide between the C-suite, regional business practices and third parties to effectively combat the risk of frauds in organizations.



Transformation of Cyber Crime

The last decade has seen cybercrime evolve from an IT issue to a boardroom concern, mirroring the digital transformation of the global economy on the macro level and of business operations on the micro level. The more the business world integrates digital elements, the more likely it is that technology has or will become a pathway for crime. While certain incidents are more likely to involve a large cyber component, cyber intrusions cause at least some instances of every type of adverse event. Furthermore, even in categories of incidents where cybersecurity breaches are endemic, perpetrators also commit analog crimes. For example, cyber breaches were most likely to be a factor in data theft, leaks of internal information and intellectual property theft. But even for these transgressions, cybersecurity deficiencies played a central role less than half the time. The conclusion is clear: As with so many other silos, the one isolating digital systems and assets has broken down. Cybersecurity needs to be integrated into an organization's overall risk management strategy.

Conclusion

The findings from the *CII-Kroll India Fraud Survey* and Kroll's global research² only reinforces the need for organizations to maintain proper data governance and ensure they have appropriate data analytics capabilities that are aligned with their risk profile. Additionally, depending on the complexity of supply chains and geographical diversity, investing in more sophisticated analytical capabilities that help correlate nontraditional datasets, predict nefarious behavior and enhance outputs and reporting may be necessary to spot the tell-tale signs of risk in an ocean of internal and external information. They must also consider other creative ways to maintain sight of the risks posed by their third-party relationships and ensure that they are training employees and contractors to spot the risks and know what to do when they see them.

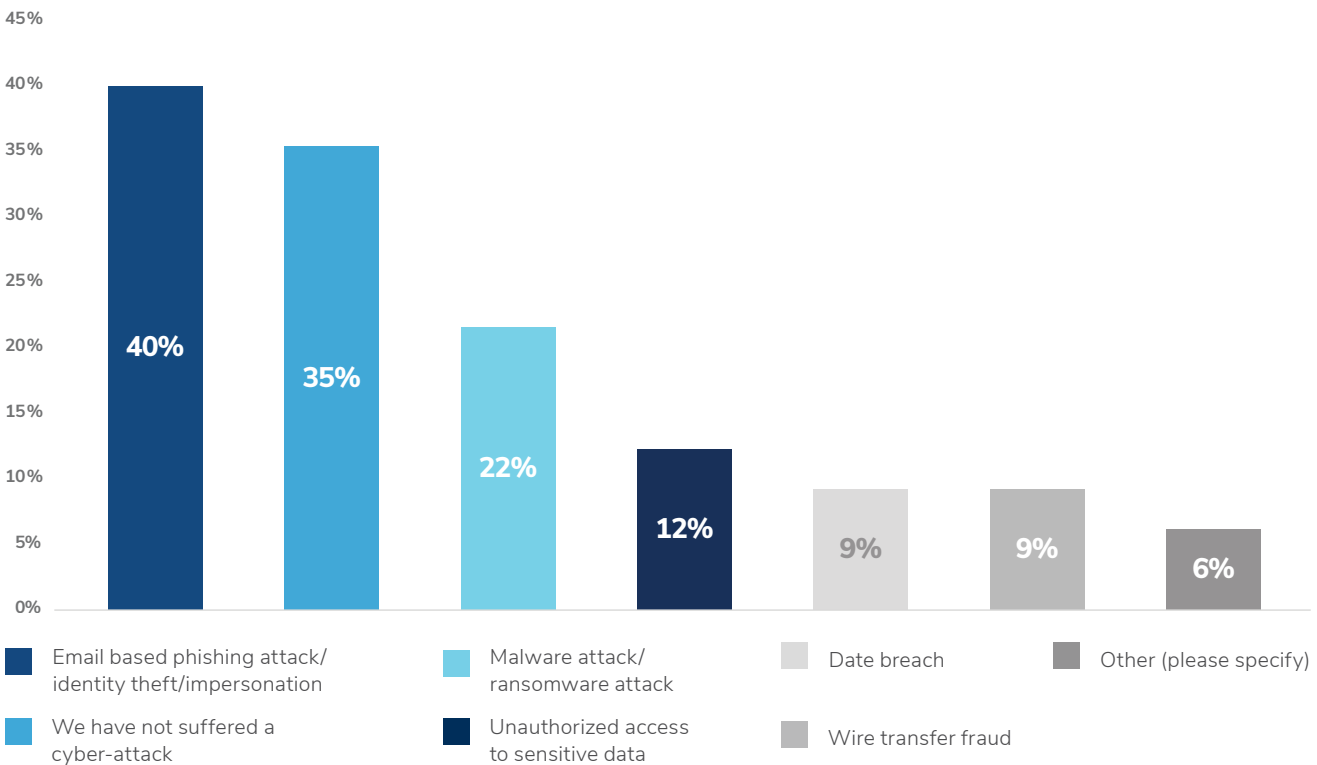
The Fraud Landscape in India: Fraudsters Go Online

Workers weren't the only ones to stay at home during COVID-19 lockdowns. Restrictions diverted attention away from fraud and allowed it to flourish in India over the last two years, but with a marked change in nature: Fraudsters stayed home too, and the threats moved online.

In the last two years, Indian businesses have seen an increase in cyber threats, with phishing and ransomware attacks in particular growing significantly compared to 2019. This is not thought to be linked to any specific aspect of the Indian market but is more a reflection on general cybercrime trends: Remote working has seen ransomware attacks increasing 148% worldwide.³

Two fifths of respondents, meanwhile, reported phishing, identity theft and impersonation attacks. But one perhaps unusual finding is that data breaches have declined slightly since our previous study, despite the rise in employees working from home and accessing corporate systems from beyond the firewall.

Which Type of Cyber Fraud Incident Has Your Organization Witnessed?

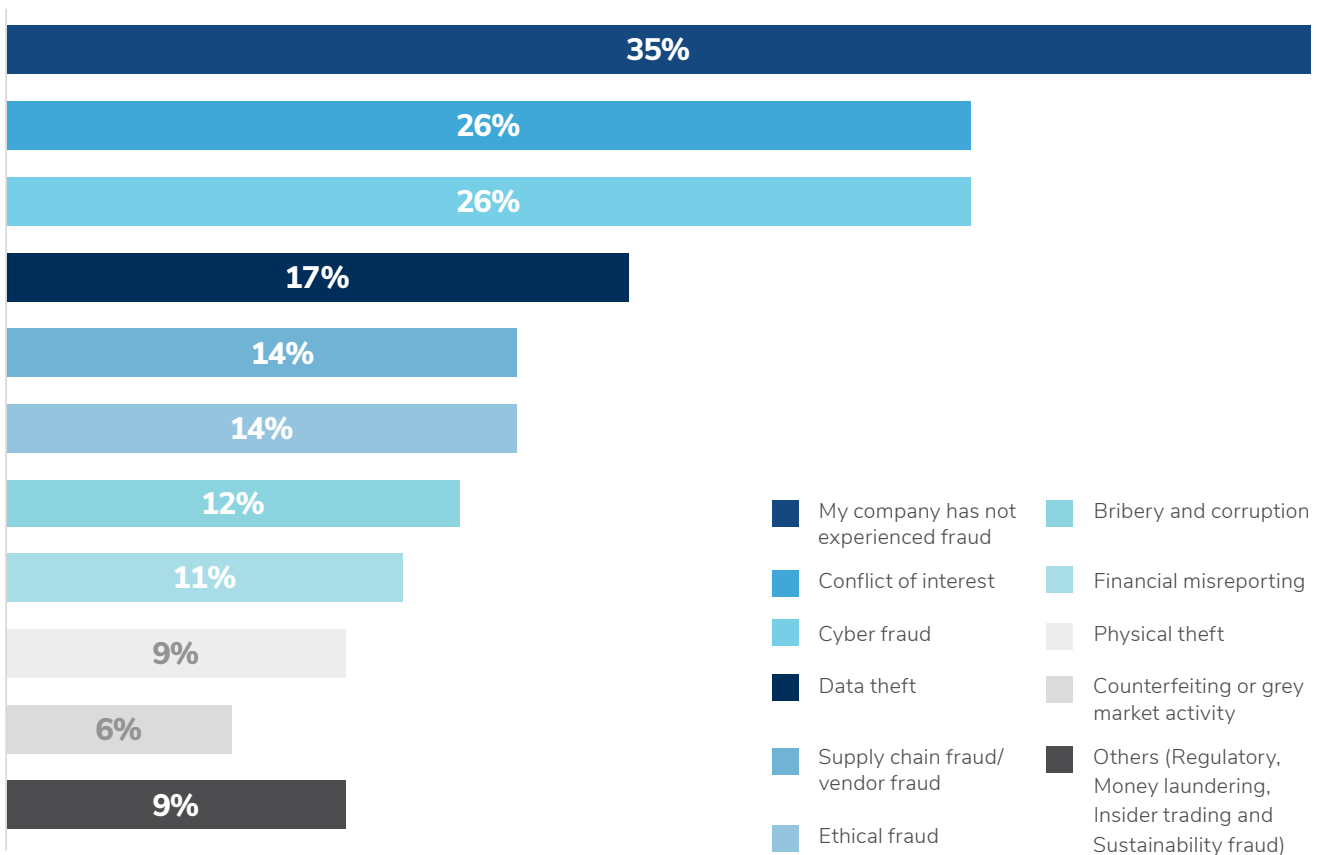


A Changing Modus Operandi

Even though management teams might have been expected to show more vigilance on account of the pandemic, in practice the proportion of companies experiencing fraud was up from 57% previously to 65% in this year's survey.

Countering the rise in online crime, and with lockdowns curtailing access to premises, physical theft was a problem for just nine percent of respondents, compared to 27% two years ago. Bribery and corruption were also down, from 31% to 12%. And reports of data theft fell from 31% to 17%, likely indicating that this type of crime is usually associated with access to physical assets such as hard drives.

What Kind of Fraud Has Your Organization Suffered During the Last 12 Months?

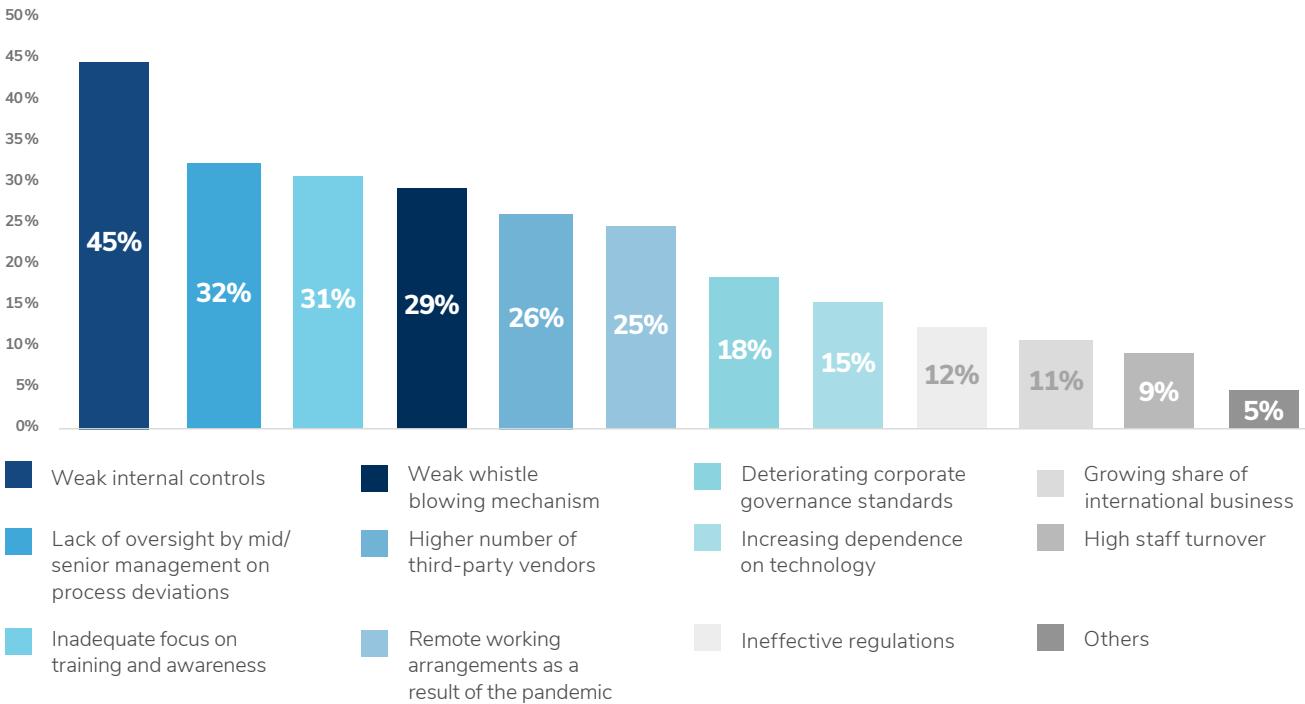


Against this, we also saw big increases in conflicts of interest and levels of supply chain and vendor fraud, which went from 10% to 26% and 5% to 14%, respectively. This appears to be a consequence of COVID-19 forcing boards to devolve operational responsibility to individuals who then used that power to appoint known associates as contractors and supply chain partners.

The survey findings are in line with the trends observed by Kroll. During 2020 and 2021, there has been an increased focus on third-party due diligence by corporates, especially when entering into new relations triggered by supply chain disruptions on account of COVID-19. Similarly, investigations reveal that more companies have witnessed collusion between senior and mid management with vendors.

Failing Oversight

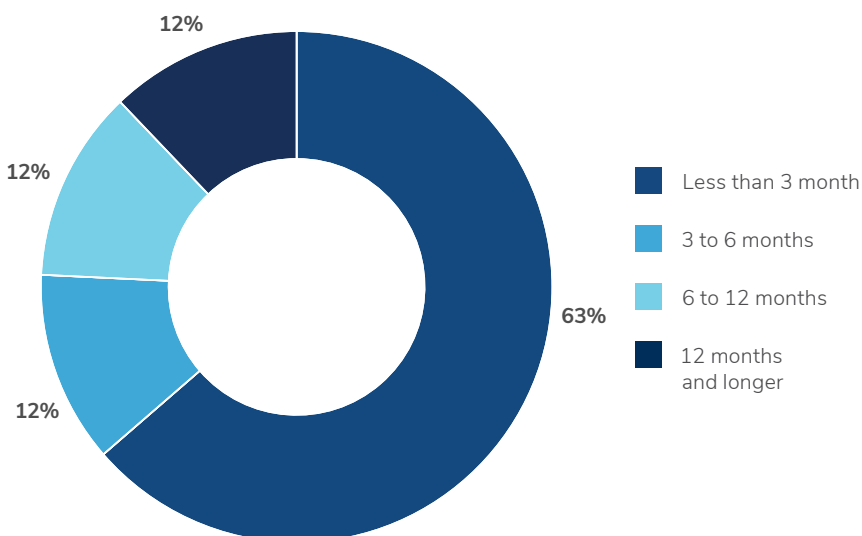
What Are the Key Triggers of Fraud?



Indeed, weak internal controls were highlighted as the main trigger for fraud in this survey, echoing a similar finding in our 2019 report. Almost half (45%) of the survey cited this factor, with a further 32% pointing to lack of oversight as a contributor to fraud.

It is important to note that the 35% of companies claiming not to have been victims of fraud may not represent the true number. Since almost a quarter of respondents said it had taken more than six months to uncover fraud, there is a good chance that criminal activity may be ongoing, undetected, in at least some of the companies in our survey.

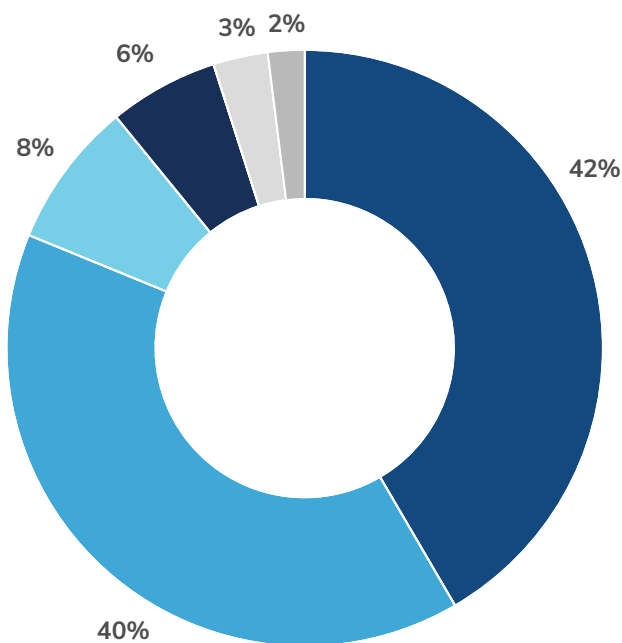
What Is the Average Time Taken To Uncover Frauds in Your Organization?



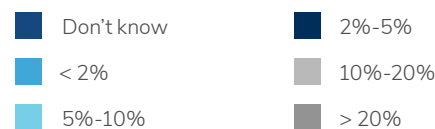
Identifying fraud in India continues to remain a challenge as many companies fail to accept that they have been defrauded. It takes multiple instances or a large event to finally react, investigate and act. Fraud investigations carried out by Kroll over the years reflect that quick response helps in minimizing losses on account of fraud and creating stronger culture among employees.

How Organizations are Tackling Fraud

Just because fraud has moved online, that doesn't mean it is any less dangerous. Admittedly, the percentage of company profits that are being lost to fraud initially looks like good news. Only two percent estimated that fraud had cost them more than 20% in profits, whereas four in 10 respondents said losses had been below 2%. But this finding is tempered by the fact that an even greater proportion, 42%, really don't know how much they have lost.



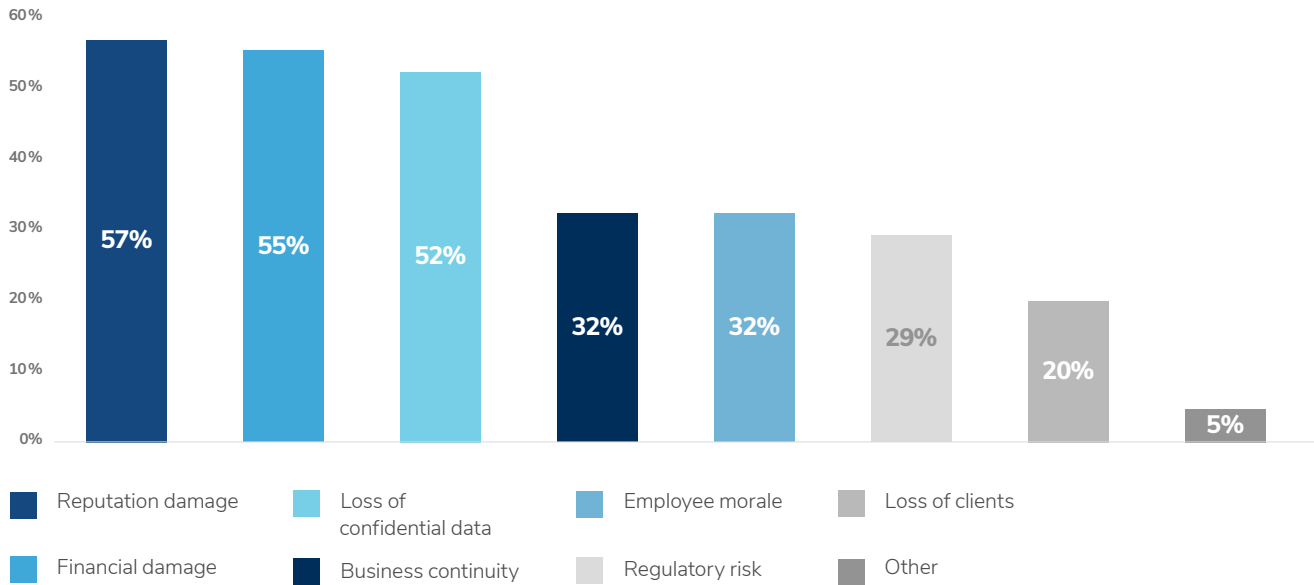
What Is Your Estimate of Loss Due to Fraud as a Percentage of Your Company's Profits?



And financial losses are only part of the problem. Our survey revealed that roughly as many executives are as worried about the reputational impact of fraud (57% of respondents) as they are of the financial loss (56%). Another almost equally big concern was the loss of confidential data (cited by 52%). As per the findings of our first survey, these impacts are likely to be correlated with company size. Larger businesses may lose relatively smaller amounts to fraud but could be more at risk of reputational damage.

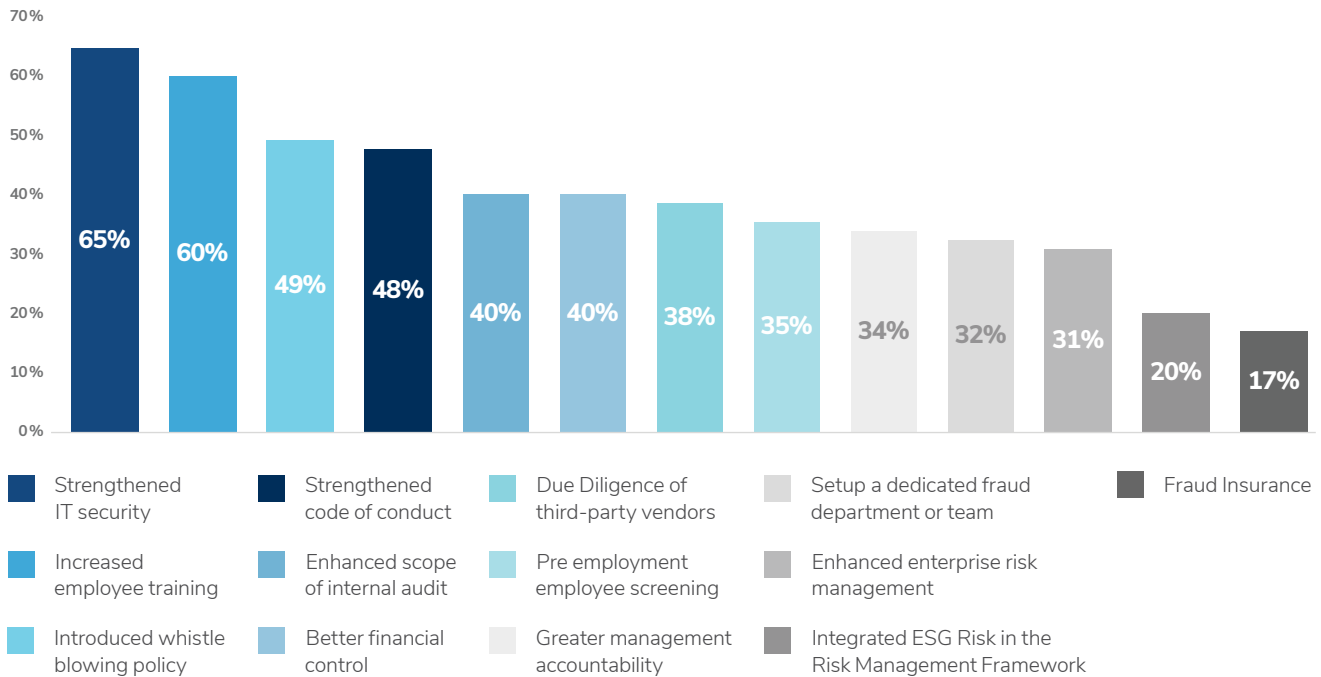


What Do You Think Is the Biggest Impact of Fraud on Your Business?



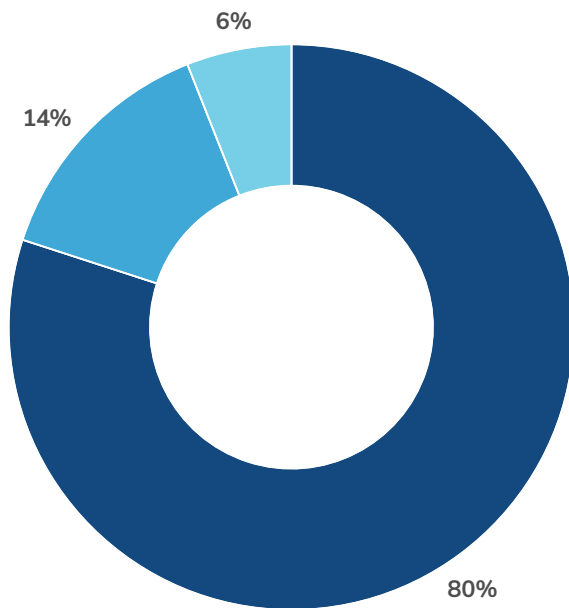
For smaller companies, meanwhile, the financial impact could be more significant. Furthermore, in 20% of the cases there was a real concern that fraud could lead to a loss of clients. Given these important effects, along with lesser threats such as impacts on employee morale and business resilience, a key question for business leaders is how to avoid and react to fraud, particularly in a more digital environment where it might be harder to track.

What Steps Has Your Company Taken to Counter Fraud?



Sensibly given the rise in online threats, the most common steps taken to counter fraud are to strengthen IT security (cited by 65% of our survey), increase employee training (60%) and introduce a whistleblowing policy (49%). Other important measures include strengthening codes of conduct, enhancing the scope of internal audits and improving financial control.

Screening Staff



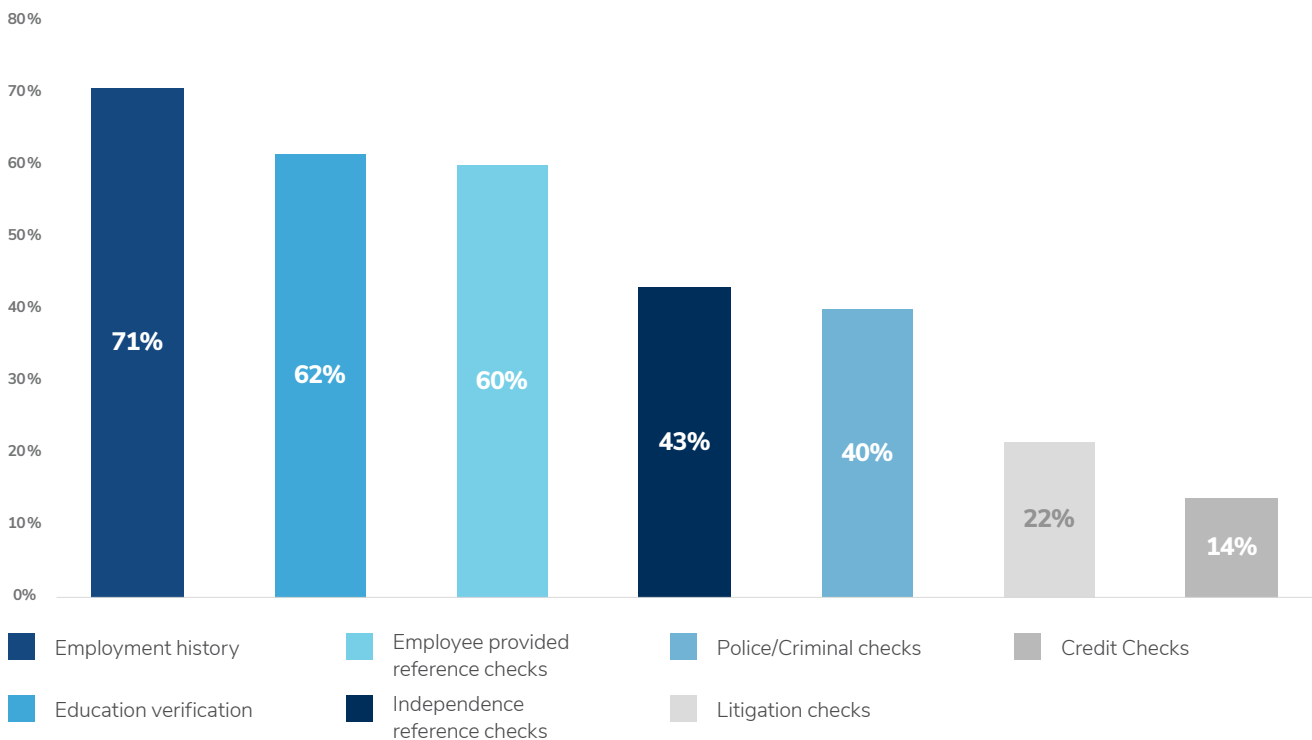
Does Your Company Do Background Checks on Employees?

- Yes
- Don't Know
- No

Kroll has witnessed an increased level of due diligence for senior roles, including board positions. Companies increasingly feel more vulnerable to a bad hire, especially on issues related to conduct, governance and culture.

When it comes to vetting employees, 71% said they checked on employment histories, 62% verified education claims and 60% took up references. But around six percent of companies do not carry out background checks at all — a level that is consistent with our last survey. Upon uncovering fraud, all respondents said that they act. The most common reactions are to report incidents to a compliance team and inform the board and internal auditors.

Which Checks Are Carried Out?

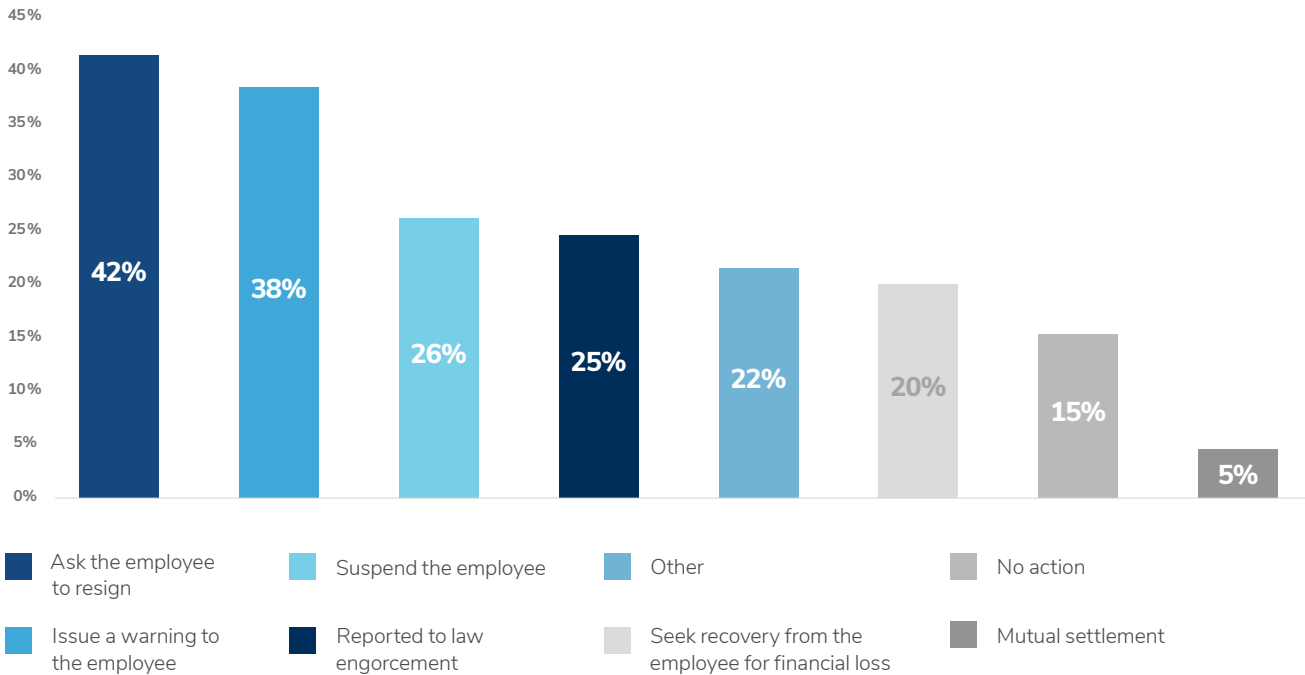


This is broadly in line with the findings from our last survey, although, respondents now seem more willing to trust internal auditors than statutory audit teams while reporting fraud. And a significant minority take things further, with 37% looking to hire an external investigation agency (compared to 27% in 2019) and 29% looking to hire a law firm (compared to 13% in 2019).

What Happens to Fraudsters?

Once they are detected, by and large, fraudsters can expect to pay. In 42% of cases, they will be asked to resign, in 38% of instances, they will get a warning, and in 26% they will be suspended. A quarter of cases get reported to the police, but surprisingly, in 15% of instances, no action is taken.

What Actions Has Your Company Taken After the Perpetrator of Internal Fraud Was Identified?



This unusual finding can perhaps be explained by the fact that in some cases criminal activity is uncovered after the culprit has already left the company, or that in some cyber frauds, such as phishing attacks, the employee is as much a victim as the business. In such situations, corporations may react not with punitive measures but by stepping up support, for instance (as seen above) by tightening IT security or improving staff training.

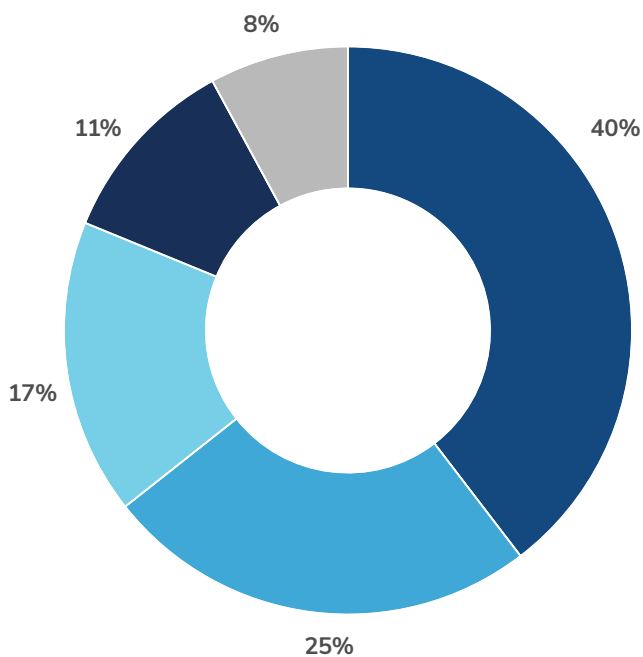
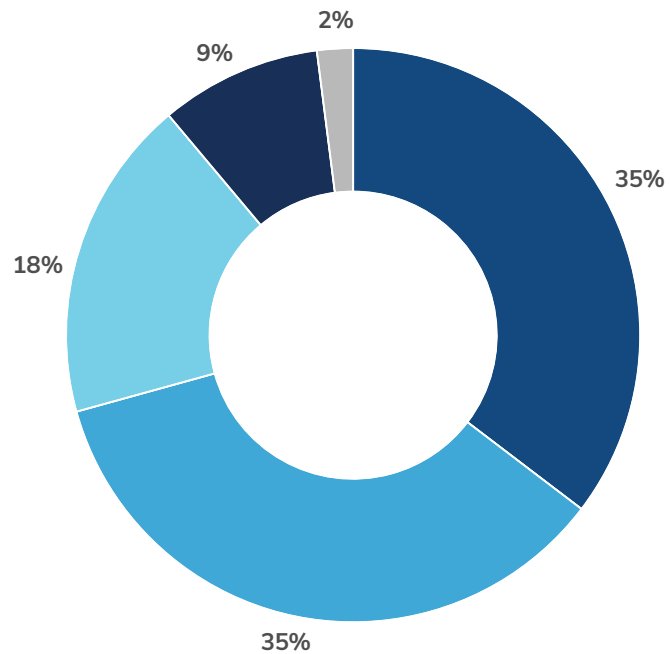


Looking Forward

The pandemic has seen communities pulling together and providing support to fight against the disease.⁴ But the community spirit has clearly not acted as a brake on fraud. Quite the opposite: With growing cyber threats, an overwhelming proportion of respondents in our survey, 70%, felt COVID-19 has increased the risk of fraud. This concern is the result of comparing current incident rates in India to those in our survey two years ago (see right).

How Much of an Impact Has COVID-19 Had on Fraud in India?

- Significantly increased
- Remained the same
- Marginally increased
- Marginally come down
- Can't say



Business leaders are clear this problem is not about to go away. More than three-fifths of respondents expect fraud to increase in the next year. What can be done to avert this issue?

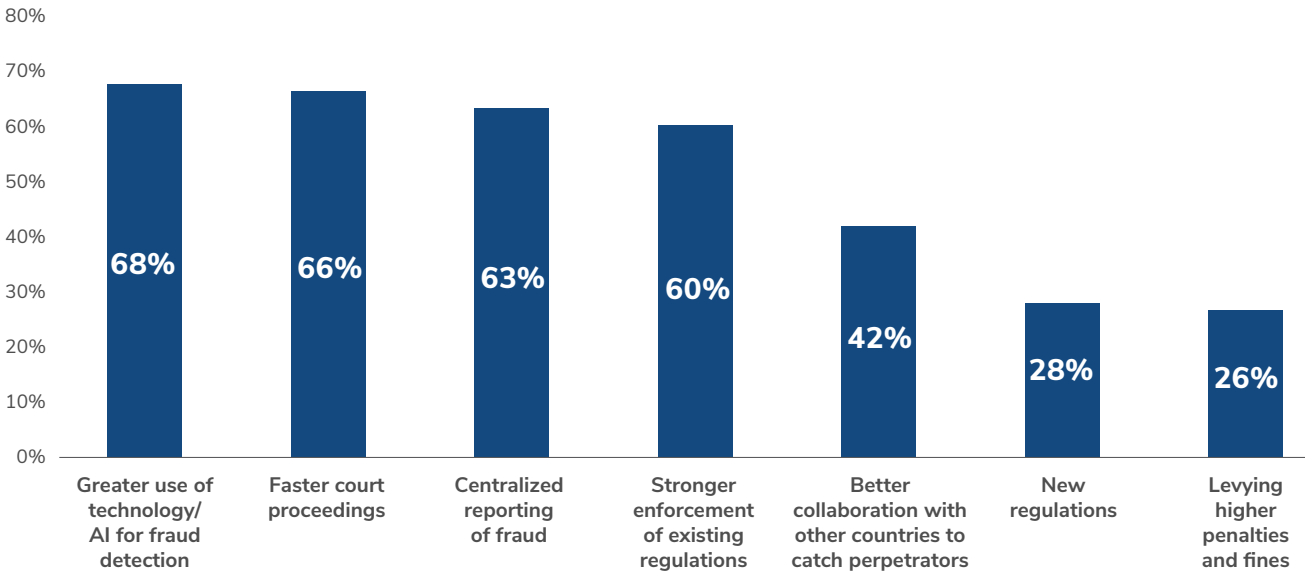
Do You Expect Fraud Risk to Increase Over the Next 12 Months?

- Significantly increase
- Remained the same
- Marginally increase
- Expect it to decrease
- Can't say

The Role of Government

The government clearly has a role to play. From a macro perspective, simply ensuring political stability has been found to have the greatest possible dampening effect on fraud, in European countries at least.⁵ In addition, our survey respondents backed a range of policy levers, with greater use of detection technology, faster court proceedings, centralized reporting and stronger enforcement all enjoying support from more than half the sample.

What Steps Can the Government Take to Reduce Fraud in India?



Espousing the use of technology to detect fraud makes sense as fraudsters increasingly go digital. In our survey, cyber fraud was the highest-ranked threat facing organizations in the future. Reflecting a rapidly evolving online threat landscape, respondents seemed relatively unconcerned with “old school” technology crimes such as wire transfer fraud and were instead most worried by the rise of malware and ransomware attacks and phishing.



A Changing Risk Landscape

Cyber fraud emerged as the most worrying threat facing Indian businesses in the future, followed by conflict of interest and bribery and corruption. The fact that these threats were seen as more critical than theft, which was also rated significantly, demonstrates the extent to which businesses will have to guard against fraud on multiple fronts.

Furthermore, when it comes to cyber fraud, the most greatly feared risk is malware and/or ransomware attacks, which can penetrate companies virtually anywhere, anytime as a result of poor employee vigilance and insufficient IT security. Data breaches and phishing attacks were also categorized as highly worrying, highlighting an emerging attack front as remote workers look to access corporate systems from across the firewall.

Vigilance is Key

What is clear in any case is that fraud in its many forms represents a clear and growing threat to Indian businesses. The only way to avoid it is to be vigilant at all levels, from ensuring digital connections are safe to maintaining oversight of business processes and divisions.

Finally, business leaders should remember the old maxim that prevention is better than cure—and seek professional advice on keeping fraud at bay rather than assuming that “it won’t happen here.”



Survey Methodology

This survey was conducted in August-September 2021 to identify the kind of fraud faced by organizations in India, the top risks organizations may be vulnerable to and what factors tend to trigger fraudulent activity. Where relevant, we have drawn comparisons with the results of our previous 2019 survey, although the multiple-choice answers were not comparable in all cases.

References

¹ Ahmad, Bashir, Maria Ciupac-Ulici, and Daniela-Georgeta Beju. 2021. Economic and Non-Economic Variables Affecting Fraud in European Countries. *Risks* 9: 119. <https://doi.org/10.3390/risks9060119>

² Kroll. (2021, September 13). Global Fraud and Risk Report 2021. <https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2021>

³ Alexander Culafi, TechTarget, April 17th, 2021: Ransomware attacks see 148% surge amid COVID-19. Available at <https://searchsecurity.techtarget.com/news/252481832/Ransomware-attacks-see-148-surge-amid-COVID-19>

⁴ Fay Bound Alberti, The Conversation, 29th April 2020: Coronavirus is revitalising the concept of community for the 21st century. Available at <https://theconversation.com/coronavirus-is-revitalising-the-concept-of-community-for-the-21st-century-135750>.

⁵ Ahmad et al.



Confederation of Indian Industry

The Confederation of Indian Industry (CII) works to create and sustain an environment conducive to the development of India, partnering Industry, Government and civil society, through advisory and consultative processes.

CII is a non-government, not-for-profit, industry-led and industry-managed organization, with over 9000 members from the private as well as public sectors, including SMEs and MNCs, and an indirect membership of over 300,000 enterprises from 294 national and regional sectoral industry bodies.

For more than 125 years, CII has been engaged in shaping India's development journey and works proactively on transforming Indian Industry's engagement in national development. CII charts change by working closely with Government on policy issues, interfacing with thought leaders, and enhancing efficiency, competitiveness and business opportunities for industry through a range of specialized services and strategic global linkages. It also provides a platform for consensus-building and networking on key issues.

Extending its agenda beyond business, CII assists industry to identify and execute corporate citizenship programmes. Partnerships with civil society organizations carry forward corporate initiatives for integrated and inclusive development across diverse domains including affirmative action, livelihoods, diversity management, skill development, empowerment of women, and sustainable development, to name a few.

As India marches towards its 75th year of Independence in 2022, CII, with the Theme for 2021-22 as *Building India for a New World: Competitiveness, Growth, Sustainability, Technology*, rededicates itself to meeting the aspirations of citizens for a morally, economically and technologically advanced country in partnership with the Government, Industry and all stakeholders.

With 62 offices, including 10 Centres of Excellence, in India, and 8 overseas offices in Australia, Egypt, Germany, Indonesia, Singapore, UAE, UK, and USA, as well as institutional partnerships with 394 counterpart organizations in 133 countries, CII serves as a reference point for Indian industry and the international business community.

Confederation of Indian Industry

The Mantosh Sondhi Centre
23, Institutional Area, Lodi Road, New Delhi – 110 003 (India)
T: 91 11 45771000 / 24629994-7
E: info@cii.in | www.cii.in

Follow us on



Reach us via our Membership Helpline Number: 00-91-99104 46244

CII Helpline Toll Free Number: 1800-103-1244

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

Kroll Associates (India) Private Limited

14th Floor, Raheja Tower
Bandra-Kurla Complex, Bandra East Mumbai, 400051
T: +91 22 6623 1000



Without limiting the rights under the copyright reserved, this publication or any part of it may not be translated, reproduced, stored, transmitted in any form (electronic, mechanical, photocopying, audio recording or otherwise) or circulated in any binding or cover other than the cover in which it is currently published, without the prior written permission of the Partners including CII and Kroll.

All information, ideas, views, opinions, estimates, advice, suggestions, recommendations (hereinafter 'content') in this publication should not be understood as professional advice in any manner or interpreted as policies, objectives, opinions or suggestions of the Partners including CII and Kroll. Readers are advised to use their discretion and seek professional advice before taking any action or decision, based on the contents of this publication. The content in this publication has been obtained or derived from sources believed by the Partners including CII and Kroll to be reliable on the basis of the survey carried out by the Partners. CII and Kroll do not represent this information to be accurate or complete. The Partners including CII and Kroll do not assume any responsibility and disclaim any liability for any loss, damages, caused due to any reason whatsoever, towards any person (natural or legal) who uses this publication.

This publication cannot be sold for consideration, within or outside India, without express written permission of the Partners including CII and Kroll. Violation of this condition of sale will lead to criminal and civil prosecution.

Published by: CII & Kroll

© 2021 CII & Kroll. All rights reserved. KR21091133