A triple threat across the Americas: KPMG 2022 Fraud Outlook

Sector Spotlight: Industrial Manufacturing

Five things industrial manufacturing executives need to know

KPMG's "A triple threat across the Americas" highlighted the overlapping fraud, non-compliance, and cyber-attack challenges that confront businesses across all sectors today. This follow-up piece reviews the dangers facing industrial manufacturing companies, and outlines five things that sector executives need to know:

01 A majority of industrial manufacturing companies experienced fraud in the last year, and their defenses are the weakest for any sector analyzed in our survey.

In the last 12 months, 60% of industrial manufacturing (IM) firms suffered some kind of fraud. Given this level of risk, current anti-fraud efforts across the sector are seemingly insufficient. Roughly one in nine industrial manufacturing executives (11%) report that their firms have no anti-fraud program of any sort; for the rest of the survey the average response here is just 3%. Conversely, comprehensive programs – which integrate prevention, detection, and response – exist at only 18% of IM firms, compared to 32% elsewhere. Perhaps most alarming, as it bespeaks a lack of attention to the danger, 60% of IM respondents say that their fraud response plans are somewhat or extremely effective, but only 46% report that their anti-fraud efforts even have procedures for responding to frauds they've discovered.

02 Industrial manufacturing firms may not appreciate the substantial fraud risk they face from company insiders.

As a group, businesses in this sector face a particular problem with internal fraud: 36% report that in the last year someone within the company – a senior manager, middle manager, or operational employee – was known to have committed such a crime. This is the highest figure for any industry in the survey.

These results are not accidental. On the one hand, IM companies reported less emphasis on internal controls than those in more heavily regulated industries. Moreover, the nature of industrial manufacturing provides important opportunities for insider-outsider collusion. For example, in the case where vendors seek to overcharge for raw materials in return for kickbacks, it may be easier to conceal such activity within the cost of manufacturing in the accounting system than in a straightforward item in accounts payable in another industry. The nature of the industrial manufacturing accounting process indicates that extra vigilance would be wise.

Consistent with this elevated threat, industry businesses struggled more than most in dealing with the fraud challenges of working from home. For example, 65% reported that such arrangements increased the risk of internal fraud because of the resultant reduction in the company's ability to monitor and control employees. Similarly, 63% agreed that "working from home has negatively impacted our ability to appropriately respond to fraud in our business." In both cases, these are the highest sector results in the survey.

Looking ahead, the survey results suggest IM companies may have a lack of awareness to the extent of the insider threat: only 28% of these respondents expect the risk of internal fraud to increase in the coming year but 48% foresee a decline – the lowest and highest figures respectively in the survey. Too many appear to be relying on apparent hope rather than effective defence: 64% say that the anti-fraud controls in place pre-pandemic have not been updated to reflect the new working reality – the second highest figure for any of the sectors covered.

03 Protecting intellectual assets and information technology systems are the most pressing anti-fraud priorities for the sector.

Cyber-attack is the most common issue, cited by 38% of industrial manufacturing firms which experienced fraud in the last year. This adds to the cyber-security concerns revealed in the survey and discussed below.

Meanwhile, for IM businesses that experienced fraud committed by an outside perpetrator in the last year, 26% report suffering from counterfeiting or privacy and 24% saw cases of IP theft or industrial espionage – the highest and second highest response rates on these crimes in the survey. Many sector companies are ill-prepared for such threats.

04 Less ready than peers for an expected compliance storm.

Industrial manufacturing companies believe that compliance risk will grow in the near future. Nine in 10 foresee an expansion in the extent of one or more of environmental, data privacy, and labour regulations in the next five years. Over that same period, 51% expect enforcement of existing rules in these fields to grow more stringent, the highest figure for any sector.

Only 52% of industry respondents, however, report that their businesses achieve international or national levels of best practice in environmental compliance, and under half say as much for anti-corruption (46%) and anti-money laundering (45%) compliance efforts. In each case, these are the worst or second worst figures in the survey. Sector executives are also the least likely of any to say that their non-compliance prevention and investigation management activities are somewhat or extremely effective.

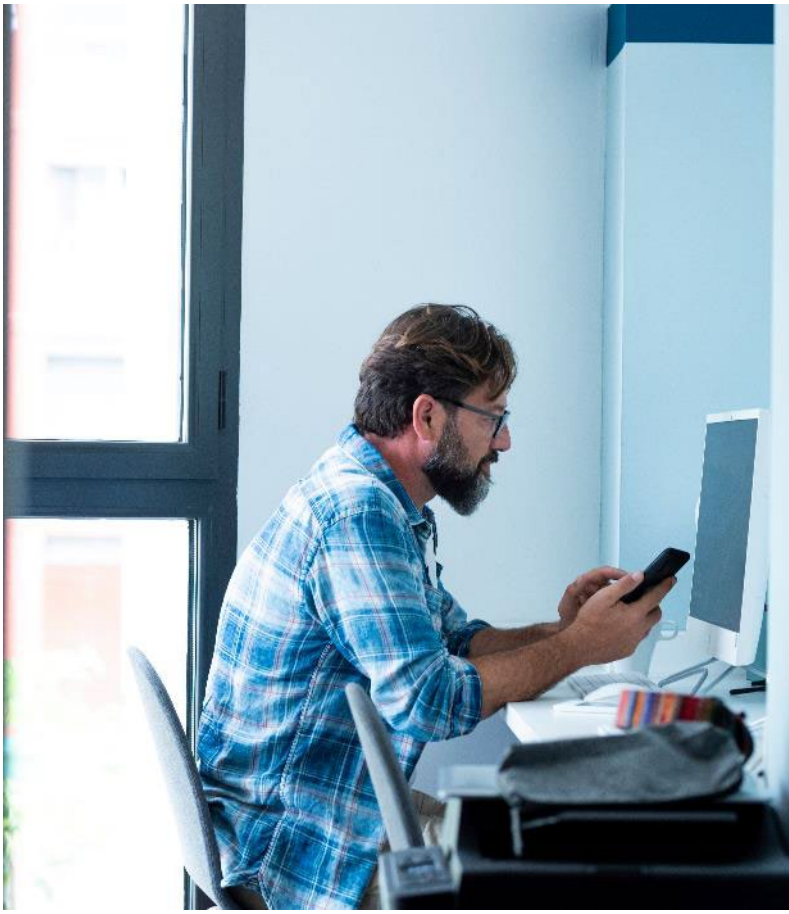
Most companies, however, do not appear ready to bolster these defences. Only 41% expect to increase spending on improved regulatory compliance efforts, the second lowest sector figure after life sciences' 37%.

05 Relatively weak cyber-security has seen further challenges as a result of greater remote working.

Just over half of industrial manufacturing companies (51%) suffered an economic loss due to cyber-attack in the last year, the highest figure for any sector. A further sign of trouble is that 75% of industry respondents say they would not be surprised to see customer data from their company leak in the next 12 months, again the biggest figure in the survey, where the average on this question was 63%. Existing defences, however, provide little reassurance: only 11% of industrial manufacturing companies can contain a cyber-attack or breach within a week of identifying it, well below even the unchallenging survey average of 19%.

Meanwhile, cyber-security is another area where the sector is wrestling with the implications of working from home: 74% of industrial manufacturing respondents agree that "remote working has been a major challenge for us in the past 12 months in terms of increased cyber-security risks" while 59% say that "our pre-pandemic playbook for cyber security is not sufficient to address risks created by the new environment in which we're operating." These are the greatest and second greatest sector figures respectively.

Amid these risks, it is surprising that the proportion of industrial manufacturing firms planning to invest further in cyber-security in the coming year (64%) is slightly below the survey average (65%).



KPMG's viewpoint: Make your defenses fit for purpose

The world is always changing but, occasionally, it experiences a dramatic inflection point. The COVID-19 pandemic reset all kinds of assumptions about how people live and work. Now, geopolitical events are exposing the fragilities of people's assumptions about the international environment.

The risk landscape that businesses are grappling with has been similarly reshaped. The need to maintain access to supplies has driven many companies to rely on previously unvetted partners, potentially raising new fraud risks. On compliance, the drive for net zero is expected to create further environmental regulation and new global sanctions may lead to more stringent oversight of financial and trade activity. Finally, cyber-attacks, already on the rise during the pandemic, are allowing cyber threat actors to pursue a range of aims.

In short, if your company has not recently conducted a full review of its fraud, compliance, and cyber security risks, it should conduct one as soon as possible. Otherwise, your defenses may not be tailored to combat today's threats, or be able to react as those risks rapidly evolve.

Unfortunately, many IM companies still need to develop the key underpinnings for those defenses while preparing for ongoing change. As our data shows, the sector has a significant internal-fraud problem. This may reflect weak internal controls relative to those in more regulated sectors – frequently in evidence at IM firms. Similarly, despite a high IP theft threat, many sector businesses lack sophisticated IP controls and too often even lack awareness of where their IP sits in the business. Finally, the low planned investment to prepare for compliance with the expected ramping up of regulations seen in our survey data fits the sector's historical pattern. Inadequate budgets in this field frequently prevent companies from protecting themselves through effective measures such as the proactive use of analytics to identify heightened risks in specific regions or functions.

For those ready to grapple seriously with the new triple threat environment, the basic framework of prevention, detection, and response remains the soundest foundation for addressing fraud, non-compliance and cyber-attack. The environment in which these defenses are deployed, however, means that they should retain the most effective elements and build upon them to defeat evolving threats.

Prevention

In our view, certain elements will remain largely the same, such as implementation or enhancement of internal controls; risk-based integrity due diligence on employees and third-parties; security assessments of critical information systems; and simulated cyber attacks to expose exploitable vulnerabilities. Others are expected to take a new shape. For example, implementing rules on exceptions to vendor due diligence policies may be necessary amid supply-chain shortages, but companies need to balance strategic necessity with the imperative to avoid falling victim to fraud and staying on the right side of regulation.

Detection

We believe tools such as data analytics, internal audits, and cyber intrusion detection protocols will remain fundamental, but the misbehaviors they look for may be different. Moreover, even where more employees are working at home, theirs are the eyes and ears that will see compliance failures or fraud. Measures that companies should take include updated training on fraud and compliance risks, and on the importance of reporting unusual behavior through existing incident-reporting mechanisms

Response

Protocols must be in place to respond to fraud, instances of non-compliance and cyber breaches. Companies also need to be ready for the emerging challenges within today's risk triangle. This might include, for example, deciding ahead of time whether you are willing to pay in the event of being hit by ransomware or choosing in advance who would make that call.

For further information on how KPMG can help you, please contact us:

Marc Miller
Partner, Advisory
Americas* and US Forensic Lead
KPMG US

Ivan Velez-Leon
Managing Director, Advisory
Forensics
KPMG US

Ana Lopez Espinar
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Argentina

Emerson Melo
Partner, Advisory
Co-Lead, Forensic Practice South America*
KPMG Brazil

Luis Preciado
Lead Partner
Risk Advisory Solutions
KPMG Mexico

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities