A triple threat across the Americas: KPMG 2022 Fraud Outlook

Sector Spotlight: Technology, Media & Telecommunication (TMT)

Five things TMT 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 Technology, Media & Telecommunication (TMT) companies, and outlines five things that sector executives need to know:

01 TMT companies face predictable fraud challenges related to their heavy use of information and communication technology, but need to remember other vulnerabilities too.

As elsewhere, fraud is a fact of life in this sector: in the last 12 months, 75% of TMT businesses experienced it in some form, slightly above the survey average of 71%. Many of these crimes reflect the vulnerabilities arising from a high IT-related risk surface. One in five sector companies suffered a fraud related cyber attack in the last year, 15% a data breach by an external party, and 15% identity theft. In every case, these were the second highest figures for any industry. TMT firms were also tied for the highest proportion in any sector that uncovered procurement fraud by managers or employees (14%). Accordingly, they cannot forget the range of possible threats while focussed on high-profile cyber-related ones.

"Fraud, cyber attacks, and other threats are on the rise. To serve the needs of customers, employees, suppliers, and society, prevention, detection, and responsiveness should be top of mind for TMT companies. Those who remain focused on these areas not only will protect their organizations' and customers' sensitive information but also will build trust and create a competitive advantage."

- Mark Gibson, National Sector Leader for Technology, Media, and Telecommunications (TMT), KPMG US

02 The sector's confidence in its anti-fraud policies may be misplaced.

TMT respondents differ little from the average in how effectively they rank their companies' performance on most anti-fraud measures covered in our survey – including financial controls, physical asset security, management controls, and whistle-blower mechanisms. They are, though, slightly more likely to say that they have somewhat or extremely effective anti-fraud policies overall (84% compared to 79% on average). They are also the most likely to give such a positive assessment of their fraud response plans (82% compared to 73% overall).

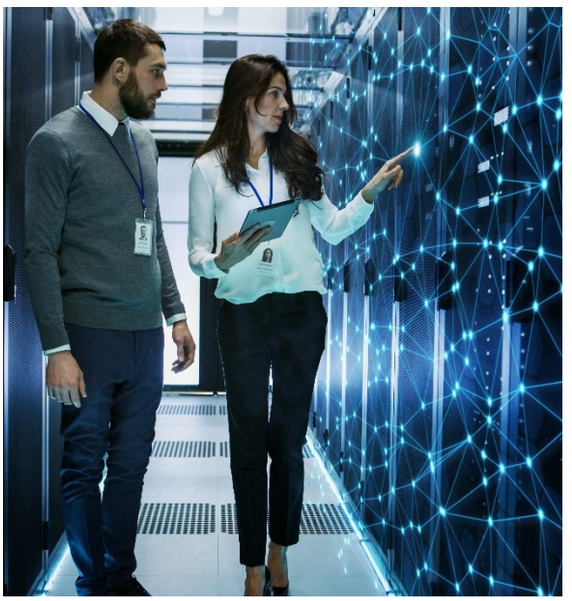
Looking more closely raises a potential red flag. One in five TMT respondents say simultaneously that their businesses have extremely effective fraud response plans and that the company has no formal fraud response program in place. Given that the sector has a slightly above average number of companies affected by fraud, and that the loss to fraud in the past year (0.47% of profits) is very close to the survey average (0.48%), such confidence in anti-fraud defenses appears unjustified.

03 TMT leaders would be well served to remember the reputational risks of non-compliance and due diligence when making investment decisions.

Sector executives do see compliance growing as a concern, but it is a less widespread worry than for peers in other industries. Overall, 53% of TMT survey respondents believe that compliance risk where they operate will rise in the coming year, and 26% foresee a decline. These are, respectively, the lowest sectoral figure seeing a bigger problem and the highest proportion predicting a diminishing challenge. Accordingly, only 51% expect that their corporate investment in regulatory compliance will rise in the coming year.

They may, however, wish to consider the reaction of stakeholders if their efforts in this field do fall short. TMT companies are the most likely to report that suppliers and customers are increasingly requiring proof of compliance with anti-corruption/AML (60%) and data privacy rules (69%). Additionally, 86% say that reputational risks related to non-compliance are causing corporate leaders to pay substantially more attention to regulatory issues at their companies. This is the most commonly cited driver of C-suite attention to compliance issues among TMT companies. Meanwhile, for survey respondents overall, only 72% say that concerns about reputational risks are increasing attention to this area.

04 Sector cyber-defenses seem insufficient in the face of a growing, and increasingly diverse, challenge.



Among TMT respondents, 83% saw an increase in the frequency of at least one kind of cyber attack over the past year. This was the second highest industry figure, after 87% for financial services. The range of attacks, however, was far different for TMT than other industries. Although the two seeing the biggest increase – phishing (41%) and scamming (40%) – were common in other sectors, TMT was the most likely of any to report growth in malware (30% compared to 22% on average), social hacking (23% to 17%), and SQL injection attack (18% to 11%). Looking ahead, 81% of sector executives foresee increased cyber-risk in the coming year.

Amid such risks, it is worrying that only 39% of TMT companies say that they can identify a cyber-breach or attack within a week of it taking place, and only 21% say that they can contain it within a week of discovery. On the positive side, sector executives appear to recognize the need to bolster defenses. They are the most likely to report an expected increase in the cyber-security budget in the coming year (74%, compared to 65% on average).

05 TMT actively addressed the cyber-risks of working from home, but most executives are now concerned about the ongoing challenges of hybrid working.

TMT was the only industry where every respondent reports that their company saw an increase in working from home. Nevertheless, the sector weathered the challenges better than others. For example, only 21% reported that that greater remote working reduced employee compliance with IT security measures. This was the lowest sectoral figure and only just over half of the overall 37% response rate. Similarly, 24% said that home working hampered the effectiveness of their compliance, and anti-corruption, and anti-fraud training programs – well below the 33% average.

This success reflects hard work. Looking back on the last 12 months, 63% of TMT respondents said that remote working posed a major cyber-security challenge. Two things set apart the industry's response. One was to move toward best practice in login technology – the use of multi-factor authentication. Of TMT firms, 62% adopted this for employees working from home, the highest sectoral figure. Overall, the survey average was not far behind, at 55%. Where the industry really differed was in empowering its people to reduce risk: 53% increased the depth of cyber-security training; 44% its scope; and 42% provided new security software for employees to use at home. The last two of these are the highest figures for any industry, and the first is within 1% of the top.

These efforts had some success: 67% of TMT respondents believe that their companies have "appropriately addressed the anti-fraud, cyber-security, and compliance challenges created by employees working from home." The task, however, is far from over. Currently, 60% remain concerned about the possible move to a hybrid working environment because it raises increased cyber risks.

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.

These defense systems must also work within the evolving framework of company needs. For example, dealing with cyber vulnerabilities to prevent fraud, attack and compliance breaches is not simply a matter of implementing better IT controls, important as these are. Many TMT businesses are struggling to find the balance between additional controls and heightened vigilance with the necessary empowerment of individual employees and the workforce as a whole.

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:

Juan Gonzalez III
Principal, Forensic
KPMG US

David Nides
Principal, Cyber Security Services
Forensic
KPMG US

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