KPMG

Fall outs from a pandemic: Risks from a Forensic Lens

IT/ITeS sector- Powerhouse of Indian economy

home.kpmg/in

The speed and breadth of the unfolding COVID-19 crisis is dramatically impacting lives and healthcare systems, disrupting business operations, slowing markets, and now posing the risk of a global recession. Economists are convinced that we are heading for a significant economic downturn; however, responses from governments have been prompt and various measures have already been taken to sustain the economy.

The USD191 billion[1] technology and business service sector which has in the past helped global organisations to stay ahead of the curve and keep critical business functions running during various crises, is now grappling with COVID-19 induced disruption of commerce across the globe. However, it is expected to see a significant slowdown in growth during this financial year as they deal with the uncertainties of COVID-19 pandemic.

As organisations find ways to tackle the immediate response to this pandemic through processes re-alignment, controls framework, delivery structures and client expectations, there are some imminent risks that may not be easily apparent but require a forensic lens. With all crises, come equal opportunities for both the fraudsters to innovate and also for organisations to become more vigilant - not just towards fraud induced losses but peeling the layers to find ways to stay compliant, optimise costs and sometimes monetise as a result of this 'pause' for perspective.

1. Technology Sector In India 2020-Techade-The New Decade Strategic Review- NASSCOM

Mitigating the risk of frauds in the IT/ITeS Sector

A. Employee at the epicenter

1. Leakage of confidential information

Remote working increases data security challenges, some of which could cause disruptions and lead to subsequent litigation. Remote access to organisation's server and data increases the risk of exposing confidential and sensitive information. This could either be unintentional or intentional:

a) **Unintentional leakage:** Social engineering is a time-tested modus operandi that continues to be used by fraudsters and hackers with an attractive success rate. Employees are contacted by emails, telephone or text, posing as a legitimate institute or a colleague, to lure the victim into providing sensitive client information, personally identifiable information such as banking or credit card details of customers and like

b) **Intentional leakage:** In case of voice services, amplified under conditions of remote work-from-home scenario, the access to sensitive client data can be abused by the employees for financial gains

2. Unauthorised modification of data

Remote working and inadequate controls leave master files and databases embedded in accounting systems vulnerable. It is not uncommon to find unauthorised alterations made to operating and accounting systems to make fictitious payments and siphon off funds

3. Charity scams

In any event of crises of national or global scale, organisations are known to go beyond the call of regulatory contributions towards social responsibility and donate towards social causes. Events such as COVID-19, present perfect opportunities for fraudsters to set-up fictitious entities to solicit donations for non-existing charities, claiming to help individuals, groups or areas affected by virus or contribute towards the development of a vaccine to fight the virus.

Due to paucity of time, organisations often do not conduct a due diligence on charitable organisation prior to disbursement towards such charities. There is a possibility that organisations may donate to charities that have questionable reputation/credentials or backed by political leaders or political parties where the funds may not be used for the stated purpose of the charitable institution

Mitigating the risk of frauds in the IT/ITeS Sector

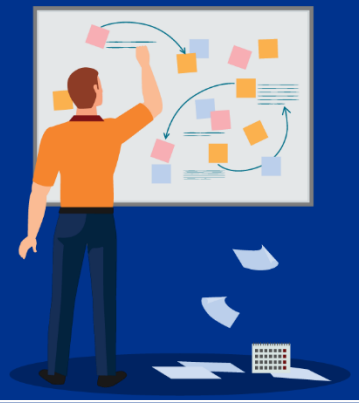
A. Employee at the epicenter

4. Weakest link in the supply chain

Several organisations have traditionally focused the most on cost effectiveness of third parties (suppliers/vendors/distributors etc.), however, current times warrant a change in approach to also focus on business continuity – both from the perspective of a vendor's capability to continue functioning as well as broadening the base of third parties for the organisation. Organisations may need to upskill their procurement teams to assess these aspects and compliance functions to be risk averse as well as pragmatic. Along with business continuity, matters such as reputational risk and regulatory compliance, continue to be equally important

5. Procurement of material and services

The current pandemic and subsequent lockdown of countries at large and resultant restrictions on imports, has magnified the lack of attention of procurement function to identify alternative sources of materials and services fulfilment. Due to unforeseen measures taken at such times in order to sustain business, controls usually fall by the wayside. This in turn could increase the risk of collusion between vendors and employees, due to reduced focus on compliance and urgency of requirement. This could potentially lead to, onboarding of favoured vendors, supply of sub-standard quality material/services by vendors at higher prices



6. Disputes

a) **Service providers:** Increase in disputes due to failure of compliance with minimum commitments in terms of number of people to be deployed, average ticket resolution, data center availability, among others could arise due to lockdown

b) **Clients:** Disputes with clients on account of project cancellation before completion of the contract period, additional cost of operation, non -receipt of fixed monthly payment, among others, could be certain challenges that the organisations face

Mitigating the risk of frauds in the IT/ITeS Sector

A. Employee at the epicenter

7. Prevention Of Sexual Harassment (PoSH) incidents

Work from home brings about a need for increased connectivity amongst team members, which may lead to inappropriate conduct by employees due to lack of/incomplete understanding of events covered

8. Anti-Bribery and Corruption (ABC) risks

During the duration of the lockdown, there is a possibility that standard processes and procedures are not followed, either to obtain or expedite the process of obtaining licenses and permits to ensure business continuity. This is especially true for organisations where third parties may act as touchpoints with government bodies

Mitigating the risk of frauds in the IT/ITeS Sector

B. Technology-driven incidents and considerations

1. Server/network access compromises

a) Using emails disguised as COVID-19 updates, fraudsters can trick the employees to handover their login credentials or click on malicious attachments/links, which will give the fraudster unfettered access to the employee's organisation's business accounts and network

b) Fraudsters can modify organisation's intranet portal to trick the employees into running malware program, which helps in getting access to their computer/server

c) Prevent organisation's customers from accessing the network by disrupting host services

2. Ransomware attacks

The fraudsters can attack critical servers and end points and lock the operating system rendering them inaccessible for the employees, until ransom is paid to the attacker (usually through bitcoins)

Mitigating the risk of frauds in the IT/ITeS Sector

C. Commercial risks through forensic lens

1. Challenges of remote working

Organisations not already setup for remote working are having to procure unbudgeted hardware and software to enable remote working. Given the time critical aspect, many organisations have gone ahead and spent on new licenses without evaluating how their existing investment could have been leveraged better. Others have scaled up their infrastructure to support remote working, without potentially factoring in additional license related costs, and could find themselves susceptible to non-compliance and unbudgeted spends (very likely at unfavourable commercial terms) in the near future

2. Non-compliance with service line agreements

Services contracts have complex pricing arrangements linked to deliverables and service level agreements (SLAs). Non-compliance with these could have an impact on budgeted revenue for work already under delivery and could lead to potential penalties

3. Open Source compliance

Open source components are being used by organisations to develop tools and products which are used for commercial purposes. Usage of certain form of restrictive licenses within these tools and products can contractually oblige the organisation to distribute the proprietary code to public. Lack of identification of such components and thereby non-compliance with its obligations might call for litigation

How could KPMG in India help?

1

COVID-19 Ethics helpline

KPMG in India are assisting organisations in setting up a COVID-19 helpline for their employees to assist in answering queries related to self-quarantine measures, overseas travel guideline, policy for work from home, lockdown etc. This helpline can be extended to offer a whistle-blower mechanism for the future.

2

Root cause investigations and impact assessment

Remotely deploy specialists equipped with sector and domain knowledge to conduct a detailed investigation into any indicators/complaints/ suspicions pertaining to potential improprieties. Our customised approach would be focused on delivering a quality outcome within the shortest possible time. This activity will enable the management of organisations to take timely corrective action and prevent any possible financial and reputational loss.

3

Pro-active data analytics

Pro-active monitoring of data and use of forensic data analytics tools developed for specific areas, such as procurement, payroll, sales and distribution spends, among others, can help identify red flags of any existing/potential wrongdoing. KPMG in India has the capability to develop a customised offering with the required inhouse tools and technology to perform the required data analytics.

4

Cyber investigations

Assist in responding to cyber threats effectively and efficiently with our bouquet of services ranging from rapid cyber incident response, containment of threat, continuous monitoring to training and capacity building, and take measures to prevent such incidents in the future.

5

Dispute advisory services

Assist in resolution of commercial and contract disputes. Provide support to your legal team by dissecting complex issues and providing robust, compelling arguments on financial, commercial, valuations, accounting aspects, timely contractual recourse taken to escape penalties, performance and invoking of Force Majeure.

6

Awareness – PoSH

As a proactive approach, assist you in re-training the staff to come to terms with the new normal and creating awareness related to the applicability and consequences of POSH by conducting online webinars.

How could KPMG in India help?

7

ABC diagnostic review

Conduct diagnostic risk review to check adherence to the defined ABC framework. Additionally, during the review, identify transactions, if any, incurred by the organisation or third parties associated with the organisation, during the lockdown period in contravention of the ABC laws and regulations.

8

Third party risk management

Assist in evaluating third parties with increased emphasis on re-evaluation of vendors, supply chain resilience, and continuous monitoring. The coverage may include matters such as reputational risk, business continuity, key person risk and others.

9

Pre employment background checks

With unprecedented economic pressures imposed by the lockdown, restricting cash flow, several marginal service providers in the employee screening space have suffered and may be finding it difficult to maintain service levels. KPMG in India's background screening practice is fully functional and innovated quickly to undertake screening through online sources and finding alternatives to verify through electronic means, for components requiring physical checks. The screening process includes verifications of key credentials of a candidate for employment, such as academic qualification, previous employment records, reference checks, and security checks such as criminal and litigation record checks, adverse web and media checks, credit checks, global sanctions and regulatory database checks, substance abuse screening, etc.

10

Software asset management

Assist to determine the requirement of software licenses in order to mitigate any potential non-compliance resulting in unbudgeted spend, as well as cost optimisation opportunities can be identified and realised. Perform a retrospective assessment of licensing implication due to changes in infrastructure.

11

Contract reviews

Review and validate pricing and billing mechanisms in clients as well as supplier contracts. This includes analysing complex, often SLA linked pricing models to determine whether all charges have been invoiced to client, as well as any potential obligations which the service provider might end up incurring due to non-compliance with SLAs and commercial terms, likely caused by unanticipated disruption due to COVID-19.

12

Open source compliance reviews

Review codes to discover non-compliance with the organisational policy and philosophy of using open source components. This also includes review of existing policies and create a reference decision tree to assist software developers to identify the categories of risk associated with the use of restrictive and/or combination of restrictive and permissive open source licenses.

KPMG in India contacts:

Vijay Chawla
Partner and Head
Risk Advisory
T: +91 80 6833 5509
E: vschawla@kpmg.com

Jagvinder S. Brar
Partner and Head
Forensic Services
T: +91 124 336 9469
E: jsbrar@kpmg.com

Ritesh Tiwari
Partner
Forensic Services
T: +91 124 336 9473
E: riteshtiwari@kpmg.com

Manoj Khanna
Partner
Forensic Services
T: +91 80 6833 5519
E: manojkhanna@kpmg.com

home.kpmg/in

#KPMG josh

home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.