TIPS – Trade secret Information Protection Strategy

Strengthen your organisation's competitive edge by protecting trade secrets

March 2017

KPMG.com/in

Understanding the realm of data within an organisation

Data as a valuable asset

The criticality of data has undergone a metamorphosis with the advent of knowledge-based businesses. The ability of an organisation to leverage data and transform them into valuable know-how has become one of the key factors for sustainable competitive advantage. However, the growing incidents of cyber crime has placed additional responsibility on organisations to safeguard their critical and sensitive data. The loss of confidentiality of such data could have a detrimental effect on the businesses such as revenue loss or loss of capital value of the organisations.

According to the Cybercrime survey study, conducted by KPMG in India in 2015, nearly 55 per cent of the companies face the issue of theft of Intellectual Property (IP)/sensitive data due to cyber crime.

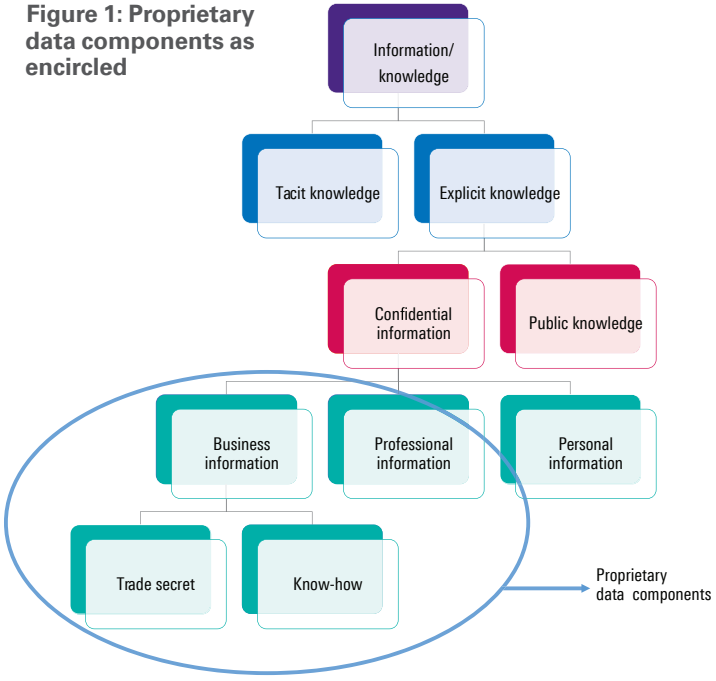
As a result, organisations have embraced new technologies in relation to collection, management, retention, and interpretation of data. The publication herein focuses on the different components of data within an organisation, establishes the importance of protecting critical data components, and the legal recourse an Indian organisation can opt for during incidents of leakage or cyber theft

Unfolding the 'critical data' jigsaw

Organisations usually deal with various forms of critical data. One of the most valuable being **'proprietary data'**, i.e., exclusive data within its domain. Since such data derives an independent commercial value, it is of paramount importance to adopt suitable measures for preventing any leakage of such data. The constitutents of propritetary data are illustrated in Figure 1, which are mainly **'trade secret'**, **'know-how' and any 'professional information'** which adds monetary value to the organisation.

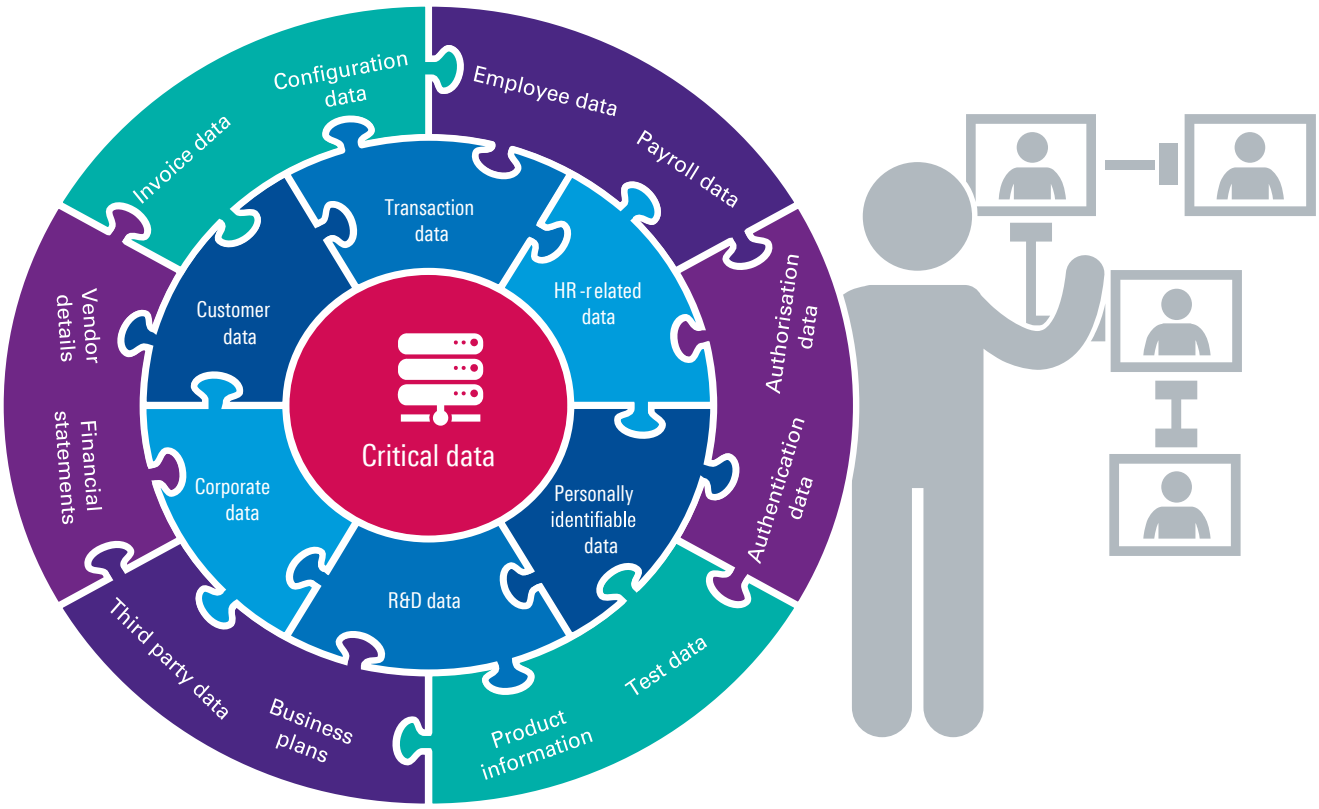
Further, following the emergence of social media, 'third-party data', i.e., data collected by the organisation, or entrusted to the organisation by third-parties also needs to be protected. For example, during any outsourcing assignment, the disclosure of technical information by the supplier. Since the data contains the third party's confidential information, lack of suitable measures to protect such data may result in regulatory breaches. Figure 2 in the following page illustrates the forms of critical data that are targeted by the perpetrators.

Figure 1: Proprietary data components as encircled



Source: KPMG in India's analysis, 2017

Figure 2: Different forms of critical data in an organisation



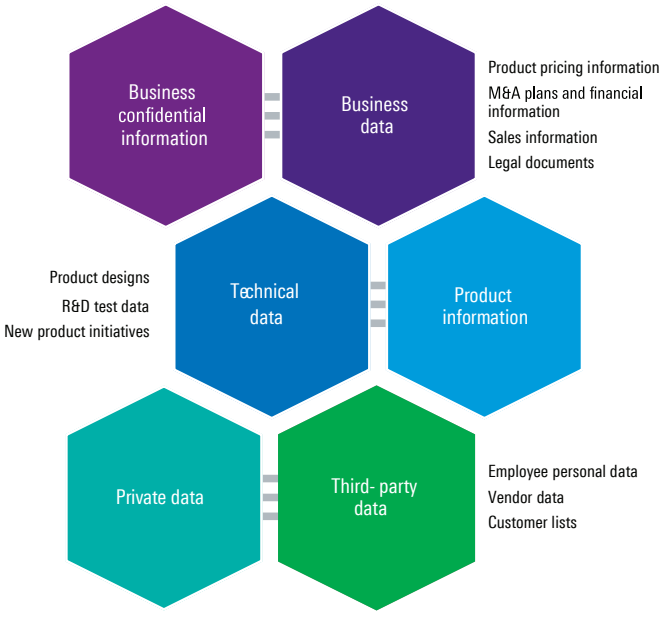
Source: KPMG in India's analysis, 2017

Decoding the meaning of trade secrets

The valuable data asset that involves substantial intellectual effort or being obtained by application of business knowledge and has an economic implication for the organisation is considered as 'trade secret'. Although it is widely believed that trade secrets are considered as confidential business information, such an assumption may not be valid in all circumstances. For instance, product pricing information is considered as confidential business information. However, if there is a unique algorithm to calculate the pricing of a product, then both pricing information and algorithm are considered and should be protected as 'trade secrets'.

Figure 3 below illustrates the different categories of trade secrets

Figure 3: Different forms of 'trade secrets' in an organisation



Source: KPMG in India's analysis, 2017

Unlike other forms of Intellectual Property (IP), trade secrets are generated when an execution and product launch plan is prepared through the implementation of tacit information. In other words, when tacit information or intellectual acumen is captured on a tangible medium, organisations can initiate their efforts to protect such collective information as trade secrets. As efforts materialise, the scope of tradesecret protection is enhanced, thereby capturing the entire knowledge base from a tacit idea to the marketing efforts made towards sale of the products developed.

Typcially, in an enterprise, trade secrets are handled by various departments. Figure 4 below illustrates the responsibilities delineated for managing trade secrets:

Figure 4: Responsibilities delineated for managing trade risks

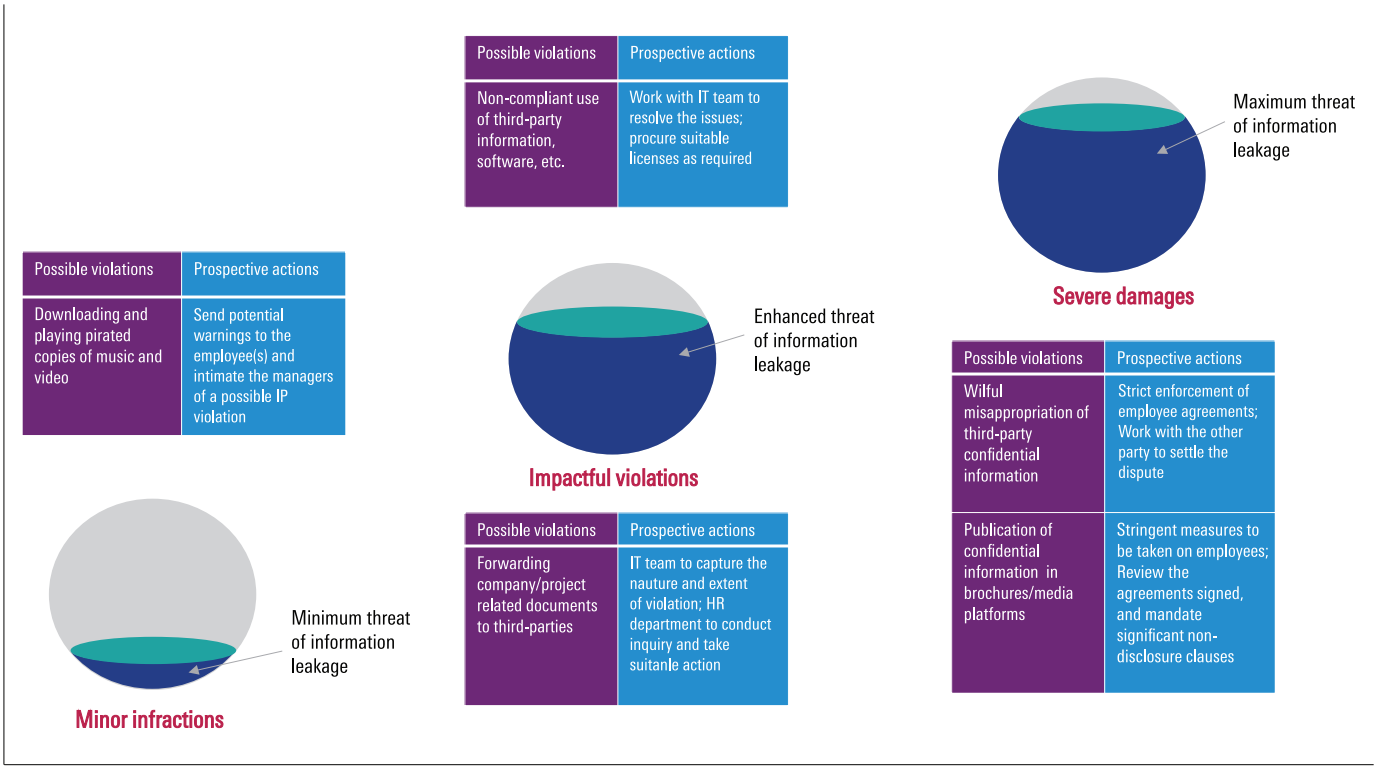
Source: KPMG in India's analysis, 2017

IT	• Implement IT controls to manage different categories of trade secrets
HR	• Record undertaking from prospective employees • Incorporate suitable clauses in employment contracts • Provide assignments and disclaimers for IPR in exit formalities
LCIA	• Include suitable clauses in agreements signed with different third parties (vendors, suppliers, collaborators, etc.) • Deploy risk mitigation measures to reduce proliferation of trade secrets • Conduct periodic audits to help ensure consistent use which is in-line with the agreements • Validate internal processes to help ensure statutory and regulatory compliance
IBU- Sales IBU - Development IBU - Procurement IBU – Quality	• Evaluate the possibility of contribution of trade secrets to the product/brand value • Develop products/solutions to manage trade secrets • Create suitable check points to ensure that vendor, supplier, and other third-party information is not leaked • Undertake adequate measures to protect quality checks, test results
R and D	• Undertake adequate measures to help ensure quality checks, test results • Select between patents and trade secrets

Additionally, the remedial measures depend on various factors, with the most critical factor being the economic impact on trade secrets.

Figure 5 below illustrates different categories of violations and possible prospective actions.

Figure 5: Trade secret violation matrix in an organisation

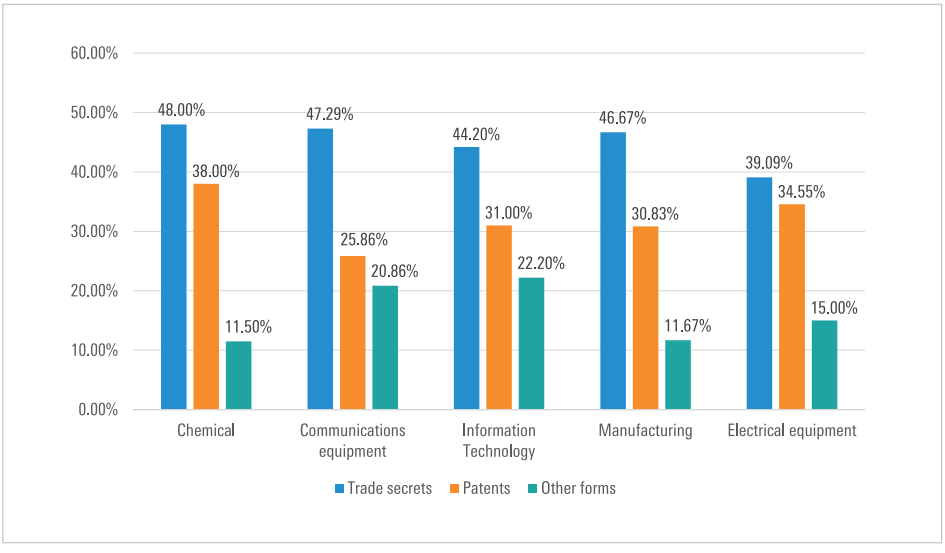


Source: KPMG in India's analysis, 2017

Protecting 'trade secrets' - A necessary evil for organisations

With the emergence of new-age technologies, trade secrets have proved to be a valuable commodity and have been instrumental in contributing to the knowledge base of modern-day organisations. They also go a long way in helping organisations achieve their business objectives. According to a study by the European Commission[1], trade secrets not only play a crucial role in protecting inventions, but in fostering innovations too. The study further indicates that organisations in various sectors have preferred trade secrets over other forms of IP protection for their innovations.

Figure 6: Preferred modes for Intellectual Property Rights (IPR protection by various sectors)



Source: European Commission study on Trade Secrets and Confidential Business Information in the Internal Market, 2013

1. http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf

The study elaborates that across Chemical, Information Technology, Manufacturing, and Comunications and Electrical equipment industries, trade secret protection has been **approximately 40-50 per cent** in comparison to patents being close to **25-35 per cent** and any other form of IPR protection being **11-20 per cent.**

With organisations essentially protecting their innovation through 'trade secrets', they constantly face the challenge of cyber theft and leakage in the public domain. Over the last few years, cyber perpetrators have been increasingly involved in devising novel mechanisms and tools to misappropriate trade secrets. Perpetrators increasingly use cyberspace and sophisticated cyber technologies to steal and transfer massive quantities of data while retaining their anonymous identity. According to the statistics published by the Ponemon Insititute, the average cost for one compromised record of proprietary data breach in India has gone up from INR3,098 in 2014 to INR3,396 in 2015[2].

According to the National Security Agency (NSA) and Commander of the U.S. Cyber Command, the loss attributable to potential IP theft through cyber espionage has resulted in 'the greatest transfer of wealth in world history'[3]. The United States Commission on the theft of IP reported that the scale of theft of IP is unprecedented – hundreds of billions of dollars per year, on the order of the size of U.S. exports to Asia[4].

Therefore, it is imperative for organisations to have a trade secret management framework to manage the persistent threat of trade secret misappropriation. Further, the framework adopted should mitigate the threats posed by different actors who can commit trade secret theft. In many of the recent incidents as observed in the industry, organisations have suffered either a direct damage or have been made victims of collateral damage due to actions of such actors. Therefore, it is necessary to deep dive into the threat actors and their activities and focus areas, as illustrated below:

Figure 7: Various threat actors and their activities with focus areas committing trade secret espionage

Nation/states

Key activities

- Acquire trade secrets and sensitive information from public officials
- Support state institutions to acquire trade secrets from regulatory bodies

Focus areas

- Military capabilities
- Economic information
- Critical scientific developments

Malicious insiders

Key activities

- Acquire corporate trade secrets
- Leak product critical information
- Leak the financial tails of critical transactions

Focus areas

- Corporate financials
- Vendor details
- Critical R&D information
- Product specific trade secrets

Competitors

Key activities

- Target corporate trade secrets individually or in cooperation with their state institutions
- Use covert means to obtain critical product information from vendors/ sub-contractors

Focus areas

- R&D and new product information
- Business plans

Hacktivists

Key activities

- Release corporate information – including trade secrets – to advance their political views
- Obtain third-party data and sensitive business information of employees
- Auction the trade secrets to the highest bidder

Focus areas

- Third-party private data
- Corporate IT information
- Employee details

Source: KPMG in India's analysis, 2017

2. http://informationsecurity.report/Resources/Whitepapers/92715d0a-7f37-45ce-974b-66cc0102b32a_2015%20Cost%20of%20Data%20Breach%20Study%20India.PDF
3. Josh Rogin, "NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history', Foreign policy The Cable
4. National Bureau of Asian Research, Report on the Commission on the Theft of Intellectual Property

Trade secret protection and legislative framework in India

Trade secrets protection is a non-statutory Intellectual Property Rights (IPR), i.e., unlike patents, copyrights, and trademarks. There is no separate legislation to protect trade secrets. The current legislative framework in India mandates that the organisations have taken reasonable measures to maintain such confidential information with economic importance as secret.

Although there is no separate trade secret legislation in India, there are various legislations which provide civil and criminal remedies on misappropriation of trade secrets. A fundamental remedy available is a common law measure of **'breach of confidence'**.

The protection of trade secrets in India has evolved through judgments delivered by various courts of India. The Indian courts have drawn extensively from English case laws, but, over the last few years, they are now increasingly relying upon the growing body of domestic jurisprudence on trade secret protection.

Table 1 below discussed some case laws which have dealt with trade secrets:

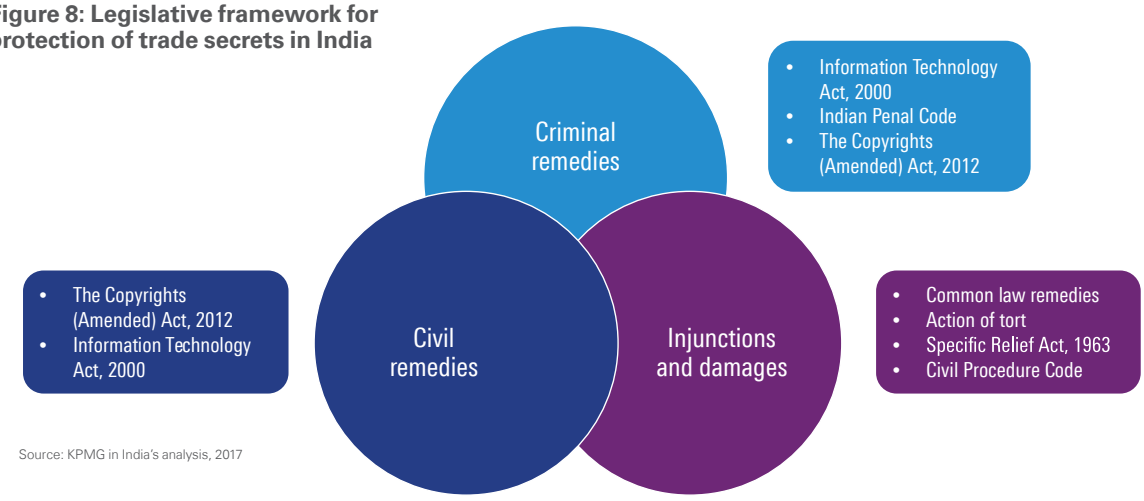
Table 1: Exemplary case examples for trade secret leakage information

Type of tradesecrets	Issues raised	Recommended approach
Third-party information	Whether information pertaining to suppliers, joint venture partners constitutes trade secrets	If such information is protected as classified information via contracts, then an action against unwarranted use may result in injunctive and equitable relief to the aggrieved party.
Technical information (product details)	Whether technical information entrusted to an employee can be defined as 'confidential information'	Technical information which the employee has acquired in the course of his employment are protected as trade secrets.
Financial information and confidential business information	Whether mere collection of data are protectable as trade secrets	A broad category of information is protectable as trade secrets as long as the information is not accessible to persons readily, has commercial value from it being kept as a secret and the owner has taken steps to protect it.

Source: European Commission study on Trade Secrets and Confidential Business Information in the Internal Market, 2013

Other remedies are contigent on the actions of threat actors, and the damage suffered by the organisations. Figure 8 below illustrates different legislations and remedial measures offered by the Indian Constitution:

Figure 8: Legislative framework for protection of trade secrets in India



Source: KPMG in India's analysis, 2017

It is time the industry builds a single approach for protecting trade secrets. The **'reasonable measures'** towards protection of trade secrets are highly subjective, and depend on the type of trade secrets, their importance to the organisation, and the threats that it may be exposed to.

Such circumstances necessitate that organisations adopt a risk based framework which can help minimise the exposure of their trade secrets. The duty of reasonable care requires organisations to adopt a strategic road map which includes a combination of administrative, process-related, and technological measures that will help them identify, classify, safeguard and protect their trade secrets. All these measures not only can help organisations create a trail for future references, incase something were to go wrong, but also to continue on leveraging their competive advantage.

Recommendations

While organisations work their way into designing the most suitable trade secret management plan of action, Chief Risk Officers and other key stakeholders are gradually realising that optimum protection of tradesceret requires a synchronised risk assesment and strong collaboration among the business, IT, HR, and third party service providers. Given the above, it is also vital for organisations to make a paradigm shift in the way strategies are designed. This could mean defining strategies based on identifying what information is at stake, rather than basing strategies on what security tools the organisation is missing. Further, it is vital for organisations to take cognisance of the following key insights:

1. People training and awareness: The human element can either make or break the organisation's trade secret protection strategy. No matter how much technology is put in to play for protecting the organisation, weakness on the people security front could negate all investments. It is imperative that organisations build a robust trade secret protection awareness programme that effectively educates its personnel and vendors alike.
2. Systematic information risk assessment: With the constant increase in trade secret espionage and its impact, it is important for organisations to identify the crown jewels that need to be protected. Organisations need to carry out the information risk assessment in depth to help ensure that right assets are adequately protected to limit impact of attacks.
3. Comprehensive information protection system: Organisations have complex IT architectures and diverse platforms to help enable their business operations. With a large threat landscape, it is essential for businesses to have an effective, predictive, detective, and corrective information protection system.

Acknowledgments

- Dr. Pinaki Ghosh
- Ritesh Tiwari
- Sumantra Mukherjee
- Priyanka Gupta
- Sriram Chakravarthy
- Iqra Bhat
- Priyanka Agarwal
- Rishabh Rane

KPMG in India contacts:

Nitin Atroley
Partner and Head
Sales and Markets
T: +91 124 307 4887
E: nitinatroley@kpmg.com

Mohit Bahl
Partner and Head
Forensic Services
T: +91 124 307 4703
E: mbahl@kpmg.com

Ritesh Tiwari
Partner
Risk Consulting
T: +91 124 334 5036
E: riteshtiwari@kpmg.com

Sumantra Mukherjee
Director
Risk Consulting
T: +91 124 334 5007
E: sumantram@kpmg.com

Dr. Pinaki Ghosh
Senior Advisor
Risk Consulting
T: +91 124 334 5232
E: pinakighosh@kpmg.com

KPMG.com/in

Follow us on:
kpmg.com/in/socialmedia