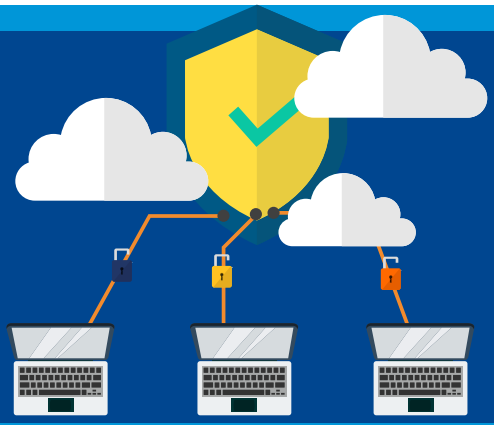
Physical security advisory services

Securing your organisation's future

August 2018

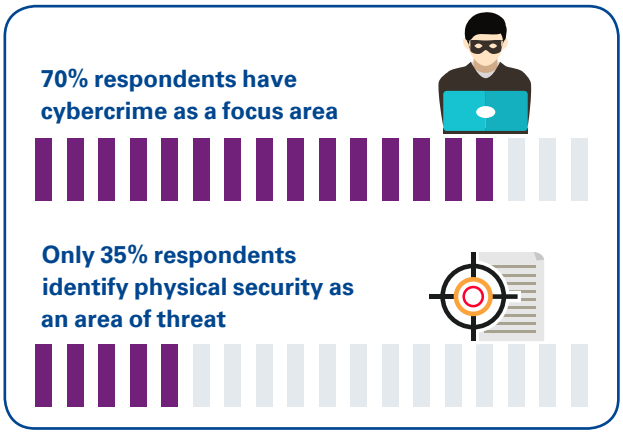
KPMG.com/in

Physical security threats on the rise



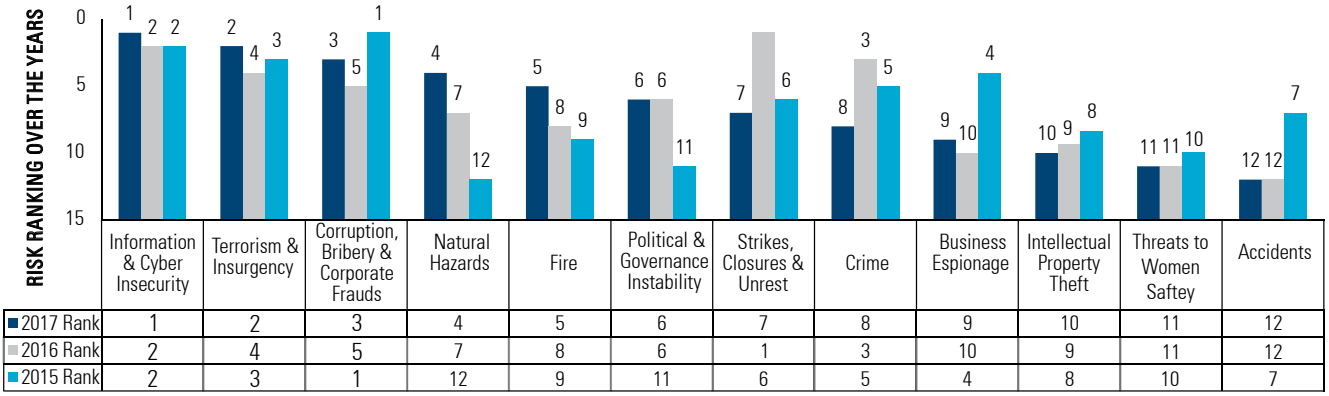
In a dynamic geo-political, economic and social environment, businesses are exposed to significant and ever-evolving risks. Organisations need to take a holistic approach toward physical security risk assessment and mitigation. More often than not, businesses nowadays plan to prepare for digital threats but not adequately prepared for the physical security threats they are exposed to.

Physical threats range from natural disasters, violence and crime to health and safety. They can be internal such as fire, workplace violence and misplacement of sensitive data by employees, or external, for instance natural disasters, theft, or utility outages.



Source: KPMG in India analysis

A glance at the India risk survey 2017 by FICCI-Pinkerton giving an overview of degree of various risks an organisation is exposed to:

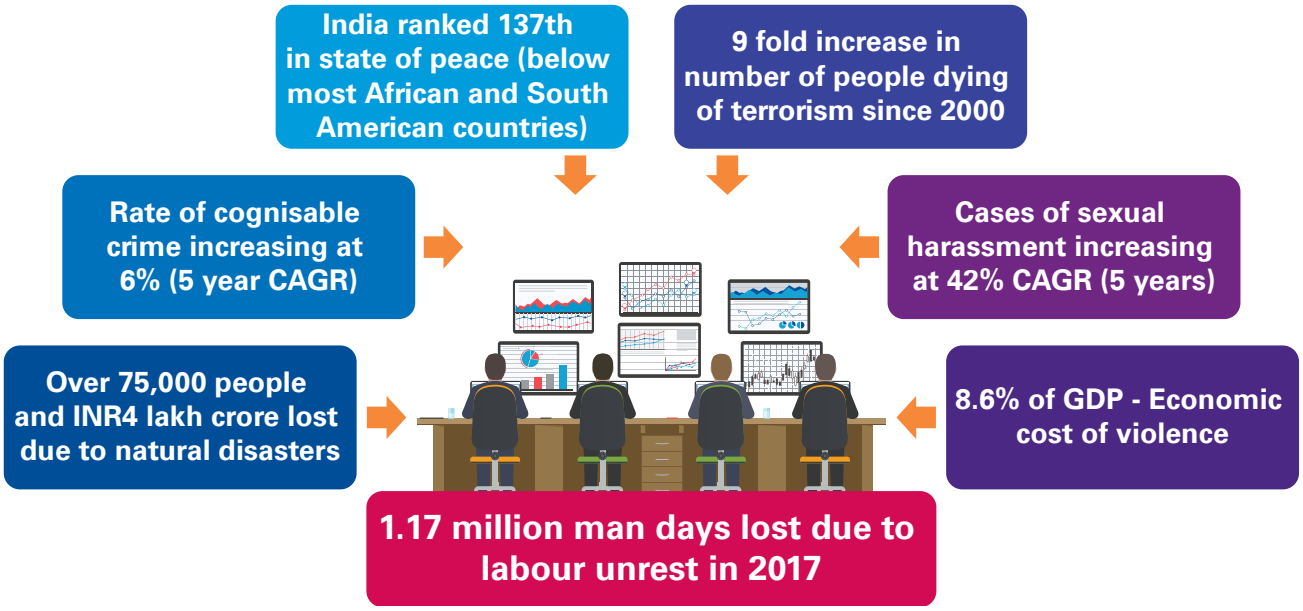


	Information & Cyber Insecurity	Terrorism & Insurgency	Corruption, Bribery & Corporate Frauds	Natural Hazards	Fire	Political & Governance Instability	Strikes, Closures & Unrest	Crime	Business Espionage	Intellectual Property Theft	Threats to Women Saftey	Accidents
2017 Rank	1	2	3	4	5	6	7	8	9	10	11	12
2016 Rank	2	4	5	7	8	6	1	3	10	9	11	12
2015 Rank	2	3	1	12	9	11	6	5	4	8	10	7

Source: India risk survey 2017, FICCI-Pinkerton, June 2017 (accessed on June 2018)

It affects your business more than ever

Physical security threats have multiple adverse effects on organisations with varying degrees of severity, ranging from business interruptions and property loss, to legal complications, reputational loss and possibly, even a shut-down of business. These factors have impacted businesses throughout India making physical security an imperative business process in an organisation.



Source: Terrorism Index, Global Peace Index, Live Mint

Our service offerings

1. Physical security assessment

- Assessment of the "As-Is" and planned security state of infrastructure
- Review of existing policies, procedures, processes, work practices and skill requirements
- Benchmarking the assessed results with established global standards
- Development of threat map
- Evaluation of risks emanating from threat analysis and development of mitigation plans
- Creation of an implementation road map
- Perimeter security, access controls, security of IT infrastructure, video analytics, transportation security, command and control centre, etc.

2. Integrated security project management

- Assessment and development of Business Requirement Specification (BRS)
- Contractual due diligence
- Bid management assistance
- Assistance for development of System Requirement Specification (SRS)
- Development/amendment of security policies and procedures post implementation of security controls
- Development of training material and implementation of training programme
- Monitoring and audit
- Post-implementation support

3. Crisis management and emergency response

- Simulation of current emergency response programme
- Hazard and risk identification and analysis of current mitigation plans
- Analysis of gaps between ideal state and current state
- Basis gap analysis, preparation and validation of emergency response and business continuity plans
- Identification of assistance required from specialised external sources
- Incorporation of validated plans into organisational management structure
- Providing specialised assistance during emergencies (if required)

4. Electronic counter surveillance

- Identification of area(s) of interest for conduct of electronic counter surveillance
- Sanitisation of the area(s) of interest for presence of electronic devices to prevent leakage of sensitive information
- Examining the source of surveillance

5. Fire and safety audit

- Simulation of fire safety drill
- Independent audit to identify gaps
- Overlay the results from the simulation with the gap analysis
- Benchmarking the output with compliance requirements, regulations, codes and standards required for providing a safe environment
- Providing a mitigation plan and implementation roadmap
- Implementation support

6. Embedded security leadership

- Identifying the requirements for security management
- Development of project governance requirements, KPIs, reporting structures and dashboards
- Deploy security management (leadership) team
- Assisting in administration and operation of the physical security function
- Coordination with key stakeholders and authorities for establishing deterrence against unlawful interference
- Management of all emergency situations
- Development of policies, processes, procedures and work practices
- Institutionalising and monitoring of training and skill-development

7. Security investigation

- Documenting the security incident
- Identification of appropriate investigation methodology
- Collation and analysis of incident related data
- Leverage KPMG network and deploy proprietary tools and investigators for filling white spaces
- Provision of investigation report

8. Training and awareness

- Functional training to security personnel
  a. Security programme management
  b. Crisis management and business continuity
  c. Fire safety management
  d. Investigation/fraud examination techniques
- Awareness training to employees for observance of security protocols and maintenance of adequate personal security
  a. Security awareness training
  b. Travel safety and security
  c. Training modules for women safety and self defence

And many more...

Our risk management framework

We provide expertise, resources and tools to our clients

- Geographical layout
- Law enforcement
- Demographic environment
- Internal threats
- Emergency support infrastructure
- Mutual-aid support
- Socio-political and economic environment
- Violence and crime history

Risk management framework

Helping clients build risk resilient organisations

Focus and grow core business – allow us to build a secure environment for you...

Our key differentiators

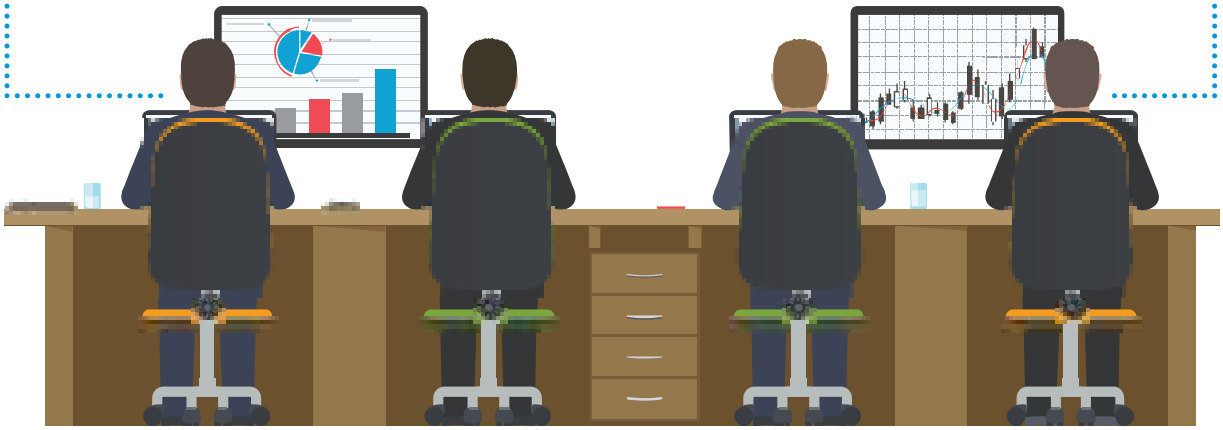
Global network and firm-wide capabilities and solutions – we leverage the capabilities of our offices across the globe and within multiple locations in India as well

Strategic focus on the security of people, assets, property, information and crisis response

'One Firm', cross-functional approach to risk

Develop security strategy, implementation and business opportunities with current leading practices driving the security industry

Continuous improvement model which is risk based and metric driven



KPMG in India contacts:

Mritunjay Kapur
National Head
Markets and Strategy
Head - Technology, Media and Telecom
T: +91 124 307 4797
E: mritunjay@kpmg.com

Mohit Bahl
Partner and Head
Forensic services
T: +91 124 336 9472
E: mbahl@kpmg.com

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

Naresh Jethwani
Technical Director
Forensic services
T: +91 80 3980 6000
E: nareshjethwani@kpmg.com

KPMG.com/in

KPMG in India 25 YEARS of making a difference

Follow us on:
kpmg.com/in/socialmedia