



Physical security advisory services

Securing your organisation's future

2022

home.kpmg/in

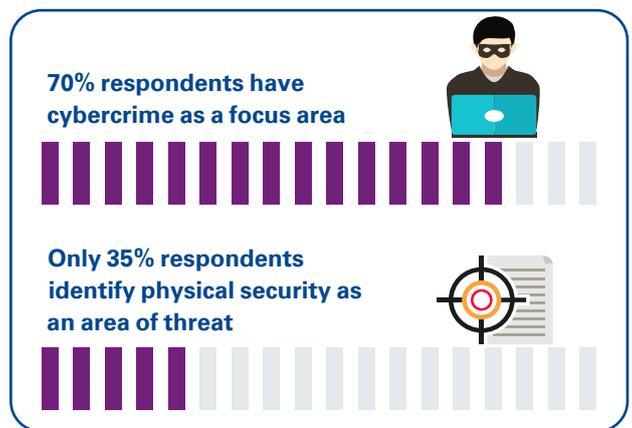


Physical security threats on the rise



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.

Irrespective of the nature of business, every business face varied physical security threats such as theft and pilferage, information theft, workplace violence, militant trade unionism, sabotage etc. with varying likelihood of their occurrence. Threat actors may be internal or external, but nevertheless businesses must realise physical security threats have varied level of consequences.



Source: KPMG in India analysis

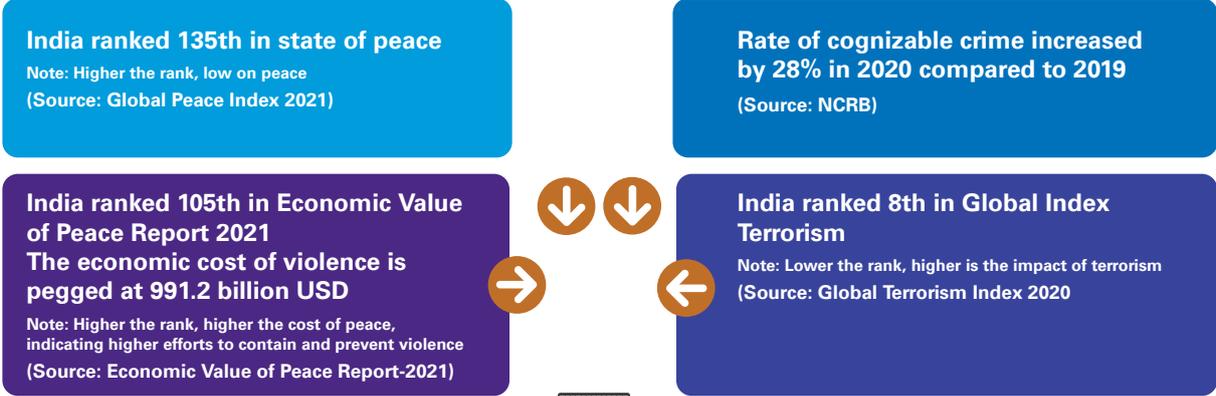


It affects your business more than ever



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.



Any risk management failure may lead to huge liability for the organisation...



...and you need to remain one step ahead

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. Security Designing for Green field and existing building infrastructure



Bridging the gap between the end-user and security technology to bring out the best Pointers are given below:

- In depth study of the infrastructure to identify physical security risks both internal and external.
- Identifying areas demanding security controls (technical such as CCTVs, Access Control Systems, Intrusion Detection Systems, Vehicle movement controls, Emergency Alarms etc. and security manpower)
- Plotting security equipment on the blue print.
- Defining the technical specifications befitting suggested security equipment.
- Identifying precise security equipment and manpower requirements.
- Dovetailing security SOPs with the proposed design.
- Integrated security project management (refer section 3 below)

- Assuring sustenance via regular assessment and audits.

3. 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

4. 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)

5. 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

6. Fire and safety review



- 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

7. 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

8. 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

9. 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

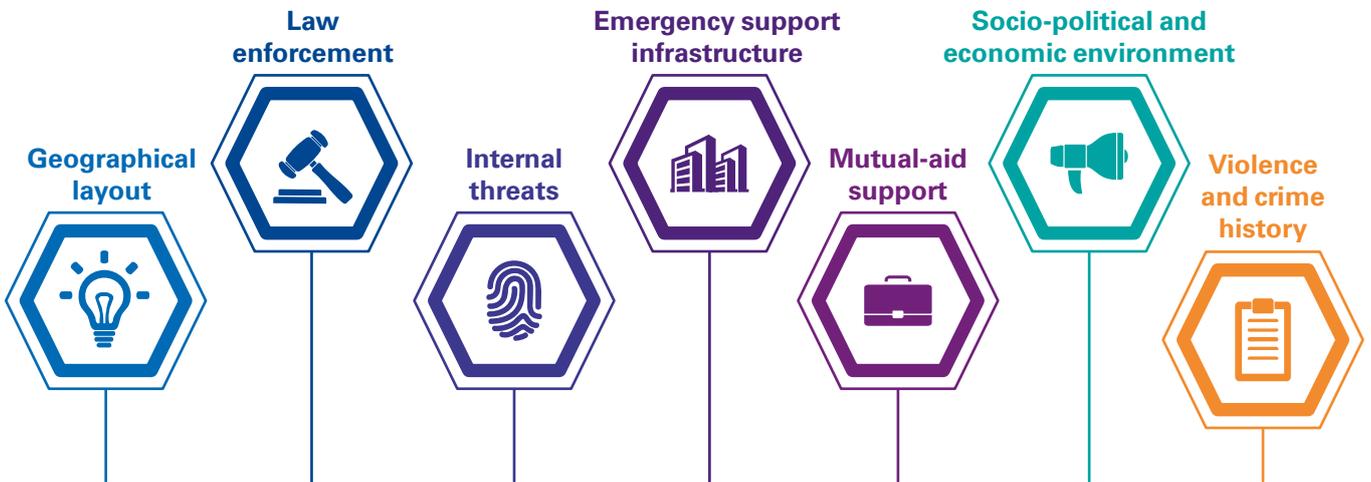
And many more...



Our risk management framework



We provide expertise, resources and tools to our clients



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



Today protection of digital assets, information security is highly integrated with physical security. KPMG with its vast range of service offerings ranging from cyber security to physical security has an edge over others for this service line.



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:

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 97 1690 9339
E: jsbrar@kpmg.com

Mitun Bhattacharjee
Director
Risk Advisory
T: +91 88 7948 6112
E: mitunb@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

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.

© 2022 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

This document is meant for e-communications only. (013_BRO0818)