Perspectives from KPMG in India

How are organisations leveraging smart physical security technologies?

February 2022

By Jagvinder S. Brar, Partner and Head – Forensic Services, KPMG in India and Mitun Bhattacharjee, Director – Forensic Services, KPMG in India

(6 min read)

Key takeaways:

- *Significant developments in smart security technologies are helping organisations address the enhanced challenges, while reducing dependence on guarding manpower. This blog focusses on such challenges faced by organisations while adopting smart security technologies*

Physical security is an integral part of the overall risk management strategy of any business enterprise. In addition to the traditional domain of security of people, prevention of theft and pilferage and protection of physical assets, several dimensions have recently gained importance. These added facets include cyber security, artificial intelligence-based (AI) video analytics, remote surveillance/monitoring and safety and security of people and assets during COVID-19-induced remote working or hybrid work model.

The COVID-19 pandemic has added two new dimensions to the domain of physical security in terms of protecting the health of employees at the workplace and also with respect to preventing contamination of products, especially in pharmaceutical organisations (other than health care sector), food delivery and entire e-commerce sector. Fortunately, significant developments in smart security technologies are helping organisations address the enhanced challenges, while reducing dependence on guarding manpower.

In the last few years, significant developments have taken place in the following smart security technologies:

- AI-based video surveillance, which can be tailormade or customised as per industry requirement
- Various biometric access control systems (facial recognition, fingerprints, retina scan, voice scan, vein scan, etc.)
- Internet protocol (IP)-based technologies
- Internet of things (IoT) and drone technologies, etc.

By integrating various inputs received from technological applications, ranging from perimeter security and other access controls to surveillance systems (e.g., CCTV, including drone inputs, leveraging video analytics, various category of sensors, etc.), smart command and control centers are increasingly reducing dependence on manpower for physical security.

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.

Challenges faced by organisations while adopting smart security technologies

- The main challenge is how to build on and **integrate existing technological infrastructure with proposed smart infrastructure** in the most cost-effective manner. This is because of challenges pertaining to interoperability of security hardware/software (incompatibility of one component with other). The complex market dynamics (presence of a large number of original equipment manufacturers [OEMs], suppliers and distributors) makes it even more difficult for organisations to choose the right technological solutions.

- Increasing **privacy concerns** also restrict the growth of the CCTV market and other surveillance devices, coupled with security concerns looming around IoT networks and cloud infrastructure. Efforts have been made globally to overcome these apprehensions by establishing the Open Network Video Interface Forum (ONVIF), founded in 2008, an international consortium that promotes interoperability of various security devices and PSIA, the Physical Security Interoperability Alliance, founded in 2008.

- Selection of **appropriate technology that is compatible with emerging technologies** like AI and robotics in a 5G communication environment, also pose a challenge. Organisations may worry that when they **invest in technology,** that particular technology should not become obsolete too soon. At the same time, they need to invest in technologies that are suitably mature and meet their requirements. Such key factors require detailed knowledge and staying abreast with current developments in security technology. Most organisations have in- house security teams, who are not well versed enough with the latest technological advancements to independently select the most appropriate cost-effective solution.

- Transcending the boundaries of technology applications by considering **integration with data analytics,** inventory controls could be monitored via linkage with existing systems for early detection of theft and pilferage. This presents itself as both, a challenge and an opportunity since it requires expertise from domains other than physical security.

- Induction of new technology solutions calls for **re-engineering of processes**, reporting channels and decisions regarding command-and-control structures. A comprehensive look at the right mix of technology, manpower, processes, and command structures can help in making the structure of physical security more efficient, reliable, and cost effective.

- In the immediate context, the challenges of the COVID-19 pandemic are going to be of paramount concern for at least another one to two years. Technological applications, particularly **video analytics and contactless access control systems**, would also require expert guidance of reliable consulting partners.

Physical security is a diverse and advanced field with its own body of knowledge. Organisations are looking to invest in new technologies to scale up and become future ready, with digital transformation as the backdrop for security infrastructure. However, from the safety and security standpoint, organisations need to assess their current technology, quality of manpower, process and organisational

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.

structure efficiently to be able to reduce human dependency and provide comfort to its stakeholders. It is equally critical to select the most appropriate security design, organisational structure and associated processes to be able to extract the best advantage of advanced security technologies in the most cost-effective manner.

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.