Hospitality: Maintaining Safety and Security during Unprecedented Circumstances

Many hotels are wondering what steps to take, in what order, to make their properties safe, and demonstrate that to reluctant customers.

In the past year, the hospitality industry has undergone a significant transformation to adapt to the changing demands of guests.

COVID-19 outbreak has presented unprecedented circumstances before the fragile hospitality industry. The highly infectious novel coronavirus continues to thwart the sector and raises serious questions about the present and future survival of the sector.

Many hotels are wondering what steps to take, in what order, to make their properties safe, and demonstrate that to reluctant customers. Hotels face the prospect of a long recovery. But the recovery will likely take longer than in other industries, and will vary across segments.

What's certain is that the next normal will be marked by structural shifts, especially around customer expectations for hygiene and flexibility.

The guest, who comes to a particular hotel, comes with an understanding that he and his belongings both will be safe and secure during his stay at the hotel. At the same time, it is also quite important that the hotel staff and assets are protected and secure.

Hence it is very important to have a proper Safety and Security system in place to protect staff, guests and physical resources and assets such as equipment, appliances buildings, and gardens of the hotel and also the belongings of the guest. Safety and Security is always the first priority towards guest service.

Vulnerability to risks faced in the Hospitality Industry

As per Ashish P. Dhakan, MD & CEO, Prama Hikvision India Pvt. Ltd., "The pandemic crises have shown the impact of vulnerability to risks faced by the hospitality industry. The hospitality industry has remained a soft target for terrorists, extremists and crime syndicates due to its close proximity to foreigners, celebrity guests and high net worth individuals for maximum impact. The previous incidents of terrorist attacks on hotels across the globe show a clear trend. The hospitality sector thrives on word-of-mouth, public perception and brand image. Even the slightest lapse in security can ruin the entire brand, not just that one particular unit.

The common serious security challenges that keep the security staff busy at hotels are thefts, fake identity, illegal activities, breach of privacy, terrorist threats, stalking, molestation, drunken brawls, etc., and accidents related incidents like drowning, fall, fire, etc. One of the newer security challenges, which has evolved is the concept of skippers – (Guests, who run away without paying the due bills). In simple terms these freeloaders con the hotel staff."

According to Aditya Khemka, Managing Director, CP PLUS, "An increase in activity always holds the potential of leading to higher risk and as the hospitality sector faces a variety of potentially damaging threats that hotels need to contend with, the overall risk rises particularly as they deal with an influx of both leisure and business travelers.

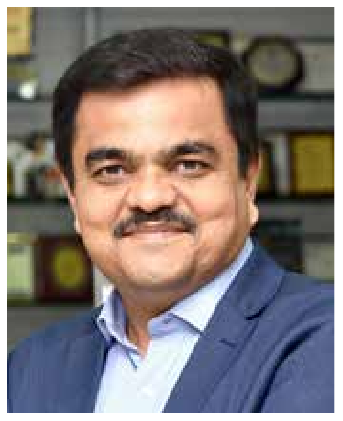
Cybersecurity has been a big concern for a number of sectors, ranging from power and utility companies to government organizations. While those specific industries are more concerned about cyber terrorism, the hospitality business is more focused on preventing data and identify theft.

On November 30, 2018, it was reported that Marriott International Inc. faced a breach that exposed the personal information of 500 million customers.

Such vulnerabilities are making the hotel and hospitality industry easy targets for hackers. As a result, every hospitality business – hotels, restaurants, reservation system vendors, and more – is facing the very real threat of a security incident. A restaurant chain with over 3,600 stores in 45 states had their customers' payment card information stolen. A breach at a global hotel group impacted more than 1,200 of its properties. Another hotel chain had two breaches in two years, with customer data once again being compromised.

'Hotels tend to be more vulnerable than other segments of the hospitality industry because of the number of touchpoints that hotel marketing processes attempt to establish with their customers. Customers make online reservations, sign up for loyalty programs that link to their cards, present payment cards for the front desk to make an imprint of, and purchase meals onsite', says Khemka.

But some hotel credit card compromises are not high-tech in nature. Many hotels still tend to receive faxed credit card authorization forms for company bookings or group bookings, and often the faxed paper forms, which contain credit card



Ashish P. Dhakan
MD & CEO,
Prama Hikvision India Pvt. Ltd.

"The physical security has remained the first layer of security despite the evolution of multiple layers of IoT driven security systems and solutions including the cybersecurity."

numbers and expiration dates, are kept in non-secure manners, such as binders behind the hotel front desk. These paper forms are susceptible to being lost or stolen.

In addition to these 'paper' breaches, the hotel industry is also vulnerable to identity thieves targeting guests who may be unfamiliar with the area or the hotel. The thieves use various schemes including calling hotel guests, posing as the front desk, asking for updated credit card information, or leaving fliers for pizza delivery with phone numbers directed to thieves who take down the guests' credit card information."

As per Kaushal Kadakia, Marketing Manager, Matrix Comsec, "Professional service, rich guest experience, and systematic hotel activities are the keys for building reputation and creating a loyal customer base. Owners of guest-centric hotels are always in search of solutions that facilitate automation of regular hotel operations. Organizations from the Hospitality Industry are oriented towards providing the finest facilities and services to their customers. This also includes the safety and security of the customers and their assets. Apart from safety measures, a good customer experience also includes exceptional services from the staff, making it a challenge for the industry to keep up.

Furthermore, security is always a point of concern in this sector. With incidents of increasing crime, security becomes paramount. For the hospitality industry, the safety of their guests and property is of utmost importance. It is, therefore, vital to deploy a security surveillance system to ensure the safety of the guests while maintaining service quality.

Again, the improper access of the employees to sensitive areas such as the server room can become a huge vulnerability for the sector as the data can be fetched and manipulated. To add to this, important data can be lost which can disrupt the regular operations."

According to Sudhindra Holla, Director, Axis Communications, India and SAARC, "The hospitality sector is a customer facing industry whose primary focus is to offer customers satisfaction and retention so as to earn their long-term loyalty towards the brand. Some of the vulnerability to risks faced in the hospitality industry are:

- **Safety and Security** - The hospitality industry has been fighting with challenge in respect with terrorism and other security risks by adapting to new technologies and training the security personnel and employees as well
- **Data Privacy** - As the hospitality sector utilizes digital systems to automate tasks and manage their data (reservations and bookings), the risk to potential cyber and data theft also increases manifold
- **Ensuring proper conduct of employees** – Property theft and misconduct can seem to pose major risks to the hospitality sector and one must ensure a proper vigilance system for continuous monitoring of staff
- **Ensuring Government issued SOPs are followed** – The new normal, as a result of COVID-19 has put forth various Government issued guidelines that have to be followed in order to ensure customer and employee safety and failing to follow a strict protocol gives birth to a number of risks
- Mostly all hotels in India have 'open door policy' inevitably introducing the risk of attracting the attention of opportunistic thieves as well as organized gangs
- One of the primary concerns in identification of unwanted individuals entering and leaving the premises. This has created a tremendous threat as the foot traffic at large hotels on any given day will vary depending on the number of events and reservations. While biometrics can solve this issue, it is not feasible to implement that as a solution for most hotel chains yet."

As per Parthesh Dhaggal, Founder, Enceplon, "The hospitality industry being the lucrative industry faces many risks. They are property theft, terrorism and shootings like the attacks in Mumbai on 26the November 2008, armed robbery, public and political violence, food poisoning, fire, identity thefts, data thefts, credit card frauds, cyber terrorism, lack of cybercrime awareness, unauthorized visitors and parking area theft.

Keeping guests safe is a high priority for the hospitality industry. However due to the difficult economic environment many businesses have scaled back on security, which can result in increased exposures and heightened liability if it creates an unsafe environment.

Guests can also pose biggest threats – both directly and indirectly – to profitability. Lawsuits from people who are injured or damage to guestrooms can represent a big risk to the bottom line.

Staff is another critical risk. During the recession, many employees were rooted in their jobs because it was so difficult to find work elsewhere. As the economy improves, staff will have more options both in and outside the industry. This means hotels are at greater risk of having their key personnel poached by their competitors. Hiring and retraining are options, but they come with additional expenses."

Significance of Physical Security in the Digital Era

As per Dhakan, "As far as today's physical security management trends are concerned, there is a seamless convergence between physical and digital (IP-driven) protocols and systems. The physical security has remained the first layer of security despite the evolution of multiple layers of IoT driven security systems and solutions including the cybersecurity.

In the good old days, security in the hospitality sector had only one connotation i.e. manned guarding. The head of security of a hotel used to be a chief of a set number of security guards. The advent of electronic security has changed physical security management in a huge way. The paradigm shift from manned guarding to electronic security has paved the way for newer positions such as Chief Security Officer (CSO) and Chief Information Security Officer (CISO). The new two-tier security structure (CSO and CISO) is now being practised in the Hospitality sector across the globe. While the CSOs' mandate remained to ensure the physical security protocols to be followed for guests, hotel staff, and vendors - besides keeping track of video surveillance, intrusion alarm and access control data, the CISO focuses on the data security and cybersecurity agenda for the hotel management, guests and staff."

"'Combating modern threats requires intelligent applications that can rapidly sift through overwhelming amounts of data that cannot be processed at the human level. Recent developments in artificial intelligence and signal processing can help security catch up. As tools become more sophisticated and readily available, security organizations must adopt new practices and capabilities. Failure to transform will increase the likelihood of becoming a target. Yet, physical security is at the core of any security system as it is about keeping your facilities, people, and assets safe from real-world threats. It includes deterrence, detection of intruders, and responding to those threats', says Khemka.

Most people think about locks, bars, alarms, and uniformed guards when they think about security. While these countermeasures are by no means the only precautions that need to be considered when trying to secure an information system, they are a perfectly logical place to begin. Physical security is a vital part of any security plan and is fundamental to all security efforts - without it, information security, software security, user access security, and network security are considerably more difficult, if not impossible, to initiate. Physical security refers to the protection of building sites and equipment (and all information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Aditya Khemka
Managing Director,
CP PLUS

> "Even if you utilize cloud-based platforms to run back-ups and provide a degree of separation or protection, your digital data is still sitting on a real-world server somewhere."

The physical plant must be satisfactorily secured to prevent those people who are not authorized to enter the site and use equipment from doing so. A building does not need to feel like a fort to be safe. Well-conceived plans to secure a building can be initiated without adding undue burden on your staff. After all, if they require access, they will receive it - as long as they were aware of, and abide by, the organization's stated security policies and guidelines.

Khemka continues, 'Despite feeling like they are in different worlds a lot of the time, your digital data has to live somewhere in the real world. Even if you utilize cloud-based platforms to run back-ups and provide a degree of separation or protection, your digital data is still sitting on a real-world server somewhere. That means that it is susceptible to all of the same problems that physical assets are within your business. It could be destroyed in a fire, corrupted in a flood, or simply picked up and taken away. So despite feeling very separate, physical and cybersecurity are intimately linked. It's something a lot of business owners don't really think about, which is the very reason why it has such a big impact. If you don't know how to protect your data against it, it's easy for cyber-criminals to capitalize on'.

The importance of protecting company information or any information from a technology standpoint is vital, but limiting access to a building can be just as effective regarding the prevention of cybersecurity threats. Due to the common availability of building security solutions becoming interlinked with one another, unauthorized individuals who have gained access to the building can use their physical access to get to a computer linked to the company's system, leading to a cyber-attack.

Hacking into network systems is not the only way that sensitive information can be stolen or used against an organization. Physical security must be implemented correctly to prevent attackers from gaining physical access and take what they want. Natural acts could include lightning bolts, floods, or earthquakes, which can physically destroy valuable data. Likewise, possible changes in quality of service by service providers, particularly water and power outage, could also serve as a physical security threat.

The best approach is to stay proactive when it comes to risk management, computer and network security, and keeping your employees safe through security awareness training, specifically on layered security."

As per Kadakia, "Physical security cannot be overlooked in the digital world. Physical security does not merely protect the premises by securing guests and personnel. Physical security devices like Access Control devices and IP cameras act as a deterrent in your absence maintaining the same level of discipline amongst everyone. This, in turn, would reduce vandalism and vulnerabilities. Introducing proper security solutions that restrict or send out notifications upon threats is of utmost importance.

Furthermore, notifying the authorities regarding threats and breaches at the right time would be too. For instance, devices like motion detectors and burglar alarms send instant notifications on predefined events. Not only the sensors but also other security devices like door security systems send instant notification to the authorities when an intruder tries to break in by getting unauthorized access."

According to Holla, "The security industry is undergoing and embracing a huge digital disruption. If the hospitality industry do not take this opportunity and utilize it to their advantage, they will end up losing out. By challenging conventional thinking and reimagining how business is done, physical security can provide next-level insights, improving life safety and creating value across the organization beyond traditional risk management."

As per Dhaggal, "Physical security is the protection of the human resource and other assets from any physical activity which may cause the damage or loose to the institute, agency or an organization. Protection in terms of physical security means protection from fire, flood, theft, vandalism, terrorism etc.

The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities and all other company assets.

The strategies used to protect the organization's assets need to have a layered approach.

Physical security is important with its main objective as to protect the assets and facilities of the agency, institution or organization. Advanced physical security measures like CCTV, intrusion detector system, cryptography, firewalls etc would be useless if somehow intruder is able to break the physical security system.

The foremost responsibility of physical security is to protect employees or human resource. Protection of employee may be from internal or external threats.

Physical security has a good number of advantages. First is perimeter security that includes mantrap, fences, electric fences, gates and turnstile. Safe locks with keys that are hard to duplicate. Badges are necessary for verifying the identity of any employee. Set up the surveillance and at places that won't expose it or let the attacker tamper with it. Strong physical security setup lowers the loss of the majority of assets, data, and equipment.

The great advantage of physical security is that criminals or attackers have to bypass through many layers of security to gain their objective. As a result, it gets harder for them to accomplish their mission. There are many methods and equipment that are difficult to scale by an intruder, has a low budget to set it and reduces security threat.

Let me enlist things that help to maintain a good and strong physical security:

- Intrusion detector
- CCTV, smart cards
- Fire extinguisher
- Guards
- Suppression systems
- Intrusion alarm
- Motion detectors
- Physical access
- Chain link fence
- RFID tags
- Barbed wire and much more

Access control (AC) are accessible to multiple operators; it includes authorization, access approval, multiple identity verifications, authentication, and audit.

Physical security plays a crucial function in protecting valuable data and information. While most cybersecurity solutions concentrate on anti-malware tools, firewall configurations, and other data security measures, however, physical security of IT resources is just as important.

While digital security is important in today's digital world, businesses can't ignore the effectiveness of physical security. Traditionally, criminals used to target physical stores. But it is now getting easier to detect physical crime,

Organisations forgetting about physical security will end up putting themselves at just as much risk. Managing alarms, sensors and CCTV should remain a top security priority alongside digital solutions.

In today's technology landscape, online and physical security go hand-in-hand, so it is important that organisations proactively protect themselves from both threats to be in a better position to combat attacks no matter how and where criminals choose to enter. Physical security are the technologies and systems in place to protect your workplace."

Security Challenges due to COVID-19

As per Dhakan, "The pandemic has created a multitude of security challenges for the hospitality sector. In fact, disruptions caused by the outbreak have emerged as one of the biggest security challenges for the hospitality ecosystem. The current security challenges in this phase are faced by the hospitality firms in protecting their infrastructure properties (Corporate Offices, Branch units, Machinery and equipment, People (Employee Health, Safety, Security & Wellbeing), Intellectual Property, (Technology, Patents, R&D and Brand), Data (cybersecurity) and Logistics (supply chain)."

Kaushal Kadakia
Marketing Manager,
Matrix Comsec

> "The improper access of the employees to sensitive areas such as the server room can become a huge vulnerability for the sector as the data can be fetched and manipulated."

According to Khemka, “The world has entered a volatile and unstable new phase. Scientists are increasingly confident that the COVID-19 pandemic threat will persist, possibly for years. The global economy is headed for an economic nosedive that could rival, even exceed, the Great Depression. With supply chains fragmenting, food supplies coming under strain, and prices rising, the lights are flashing red. Not only will this translate into rising unemployment and food insecurity, but it could quickly escalate into political unrest, violence, and conflict.

While some forms of crime have decreased, tensions are already flaring around the world, and not just in war zones. Protests, many of them violent, have broken out from Brazil and India to Kosovo, Malawi, and South Africa. Police repression is also increasing from Kenya to the Philippines. Signs of fragility are not confined to poorer countries or even to marginalized communities in wealthier cities. The yellow vests movement has taken to the streets of Paris, while armed protesters have marched on state assemblies in the US denouncing the lock-down, farmers have been living and protesting at the Delhi-UP border for months.

COVID-19 is putting hard security threats between nations back into the spotlight. The geopolitical rivalry between the great powers is likely to worsen as the American and Chinese economies become less interdependent. The next tier of major powers poses risks as well. Europe has been hit hard by the virus, once again fraying ties between the Eurozone’s stronger and weaker economies. The on-going Indo-China conflict at various spots is also posing grave danger.

At the same time, the fragility agenda that got underway during the 1990s and 2000s is going global. ‘In the past few years, the World Bank and United Nations have converged on an analysis where violent conflict is driven by a combination of failing government institutions and the grievances that fester when groups feel excluded and neglected. As the pandemic and ensuing economic crisis unfolded, these conditions have increasingly been found in many, if not most, countries in the world. This is not an agenda limited to poor countries at war but is much broader and more insidious’, says Khemka.

At the very least, the risks of violence have risen in the most vulnerable countries and cities. Keen not to let a good crisis go to waste, armed groups, terrorists, and organized criminals are already exploiting the pandemic. They will find further opportunities - including in cyberspace - once bailout packages begin to flow. Violence against women and human rights abuses have already spiked – both of which are harbingers of other forms of violence. This is set to intensify as at least 1.5 billion children and young people are sent home from their schools and universities. Many will be angry as they lose opportunities and a minority will convert this anger toward more dangerous purposes.

The Black Hat survey found that nearly 95% of security professionals believe that the COVID-19 crisis increases the cyber threat to enterprise systems and data, with 24% saying the increased threat is “critical and imminent.” The FBI backs that up: in April, the Internet Crime Complaint Center (IC3) reported that it was seeing a 300% spike in cybercrime since the beginning of the pandemic. During a webinar hosted by the Aspen Institute, Tonya Ugoretz, the deputy assistant director of the FBI’s Cyber Division, said that the IC3 was receiving between 3,000 and 4,000 cybersecurity complaints each day: a major jump from pre-pandemic levels of about 1,000 daily complaints.

Khemka continues, ‘COVID-19 has forced organizations to shift rapidly to remote working at scale. This is likely to have a significant impact on both IT infrastructure requirements and the attack surface. For example, security controls may not be applied to new systems or tools hastily stood up to support employees with remote working. Similarly, existing procedures and good practices may be side-stepped or become unavailable.’

The criminal threat actor behind Emotet, which provides malware delivery services to sophisticated criminal actors including TrickBot, Ryuk, and Dridex, began using COVID-19 phishing lures in January 2020, while the crisis was still in its early stages. Other actors have since followed suit, with hundreds of new COVID-19 themed phishing lures being created each day. Criminal and state-sponsored campaigns exploiting COVID-19 have been identified and it is anticipated that they will also use VPN and video conferencing software lures to take advantage of users unfamiliar with remote working.”

As per Kadakia, “The added security challenges due to COVID-19 for the hospitality industry primarily focuses on the safety of hotel staff and guests. The shift on increasing the security at the check-in points of hotels by measuring user body temperature has been an added challenge. Another challenge connecting to the same root, authorizing access to users who have normal body temperature.

Apart from this, minimizing the touchpoints in the premises is another security concern. Touchpoints are higher in common access areas such as elevators. Next, minimizing touchpoints at the dining space is another concern."

According to Holla, "The contribution of CCTV, as generally perceived by people as the crime prevention tool, has substantially evolved over the years. The pandemic has significantly transformed business operations affecting all verticals and even the hospitality industry, it has immobilized the global workforce to their houses and has thrown a major challenge to all business leaders in terms of business resilience and being the caretaker of the employees.

Some of the added security challenges due to COVID- 19:

- Ensuring Government issued SOPs are followed – The new normal, as a result of COVID 19 has put forth various government issued guidelines that have to be followed in order to ensure customer and employee safety and failing to follow a strict protocol gives birth to a number of risks
- **Incident response:** Have a team who can handle incidents and respond effectively. Since the risk team is now operating in completely different environments and mindsets, incident response plans and protocols might become obsolete or need to be adjusted
- **Ensuring that remote access capabilities are tested:** Security teams should ensure that company laptops have minimum viable end point configuration for remote working. Whenever possible, they should confirm whether personal devices have adequate anti-malware capabilities installed and enabled."

According to Dhaggal, "The COVID-19 pandemic has posed numerous added security challenges to the hospitality sector. They include near standstill in travel, widespread hotel cancellations, drastic decline in customer numbers, mandatory checks for all guests staff and visitors, strict enforcement of hygiene in hotels, compulsory wearing of face masks for all who enter the hotel, medical check-up like temperature, BP, etc.

Finding right partners who can provide scale, innovation and high levels of security to move more towards AI and other technology. The Covid-19 has hastened the need to use technology to allow least contact with humans. Hotels must plan now to do a soft-opening with one floor or two with only essential facilities and staff. The essential services will include housekeeping, a section of the kitchen, the coffee shop/dining room, a bar, engineering, front desk and security. This will ensure fewer people about.

The staff positioned should be experienced, multi-skilled and loyal employees. It will be a while when other regular staff will be required. All staff should continue to wear surgical gloves and masks to give confidence to the guests.

This time, the checks and screening will have to be erected for health purposes. The security will check for fever with a remote thermometer, shower a light sanitizer mist, keep hand sanitizers at the reception, elevator lobbies and guest rooms.

Sudhindra Holla
Director, Axis Communications, India and SAARC

> The security industry is undergoing and embracing a huge digital disruption. If the hospitality industry do not take this opportunity and utilize it to their advantage, they will end up losing out.

Ensure the circulation of fresh air in guest rooms and display indoor air quality. The guest room will have a sign mentioning ‘This room has been sanitized for your health and safety’.

Self-monitoring gadgets are given to guests in major hotels.

Virtual views on the TV of restaurants, lobby, and bars to see the atmosphere to avoid crowds.

Digital payments of bills and food and beverage at kiosks which will give out receipts much like the ATMs.

The number one consideration post COVID-19 will be on health and safety which translates into hygiene and sanitation issues of the hotel. The key is to provide physical evidence of the hotel’s concern for health and safety. Sick person should be isolated in a room, alone, or at least 1 metre away from others, according to local health authorities’ instructions. No visitors should be permitted to enter the room occupied by the affected guest.

Staff should also move people traveling with the sick person to a different room, if possible.

If staff develop COVID-19 symptoms while at work they should immediately stop working, put on a medical mask and isolate in a suitable room while medical services are notified.

If a staff member develops symptoms while at home, they should stay at home and seek medical attention.

Investments in technology across hospitality in the near term will be focused on solving immediate challenges and provide or bolster new business opportunities. Some of the technology that will enable this rebound:

- Online and mobile ordering
- Loyalty programs (data-driven marketing/content management)
- Remote and virtual training/ onboarding tools
- Flexible network infrastructure, edge applications
- Contactless payments
- CX (customer experience)
- AI-enabled assistants (i.e., chatbots)
- Security solutions
- Constant health and sanitation monitoring
- Clearly a short-term issue that will not impact viability.
- Focus on HR, talent and communications on providing clarity for your people, and on maintaining engagement and morale in this difficult time.
- Offering guests different options for cancellation to retain the customer in the long-term.
- So, until COVID-19 is completely eradicated the hospitality industry will have to face tough times with added security challenges.”

Technological Advancements

As per Dhakan, “The hospitality industry has come a long way from the manned guarding era, today the hi-tech hospitality electronic security systems are enabled with AI and IoT applications. It is amazing to see how the hospitality sector has become an applied field of advanced transformative technologies such as Artificial Intelligence, Internet of Things (IoT), Big Data and Blockchain. The hospitality sector has remained the early adopters of new technologies and security innovations. In India, the hospitality sector has been in the forefront of technology adoption in Video Surveillance, Access Control, Perimeter Security, Intrusion Alarm product segments. The Hospitality Sector specific products like Smart Locks, Smart Pole, Emergency Call Box, Bollards, Under Vehicle Surveillance System, Door Frame Metal Detector, Hand Held Metal Detector, X-ray Baggage Scanners are serving the special security requirements.

Integrated Security Solutions

The key transformative technologies like Artificial Intelligence (AI), Internet of Things (IoT), Big Data (Video Analytics) and Blockchain (Data security) have given a boost to integrated security solutions. The rise in proliferation of IP cameras has supported the integrated security solutions. The integrated security solutions are bolstering the hospitality security management through innovative solutions and applications, which includes advanced systems in Video Surveillance, Access Control, Intrusion Alarm, Perimeter Security segments. When these solutions are integrated with command and control center, they provide better outcomes in terms of proactive security management.

IoT Security solutions for Smarter Hotels & Guests

Internet of things (IoT) is enabling smart security trends in the hospitality sector while driving service efficiency. The hotel experience is getting a boost from IoT ecosystem. From access to streaming services to a room key on your smartphone, the essential amenities in a guest room are becoming increasingly digital. Guests want concierge services or temperature controls at the push of a button (or tap of a finger), and voice-activated controls are expanding beyond simply asking Alexa to play your favorite song. There is plenty of research to suggest that there is a growing interesting from both hospitality businesses and their customers in the potential for self-service solutions.

Physical Security Systems

There are many hotels and other properties within the hospitality industry that feel like they need to upgrade their physical security measures to Non-intrusive physical security systems. Huge barriers and barricades don't look appealing to the eye, and many worry about putting guests off. The industry trends are moving towards non-intrusive security devices and systems that are almost invisible or at the most gel with the interiors to make itself invisible.

Artificial Intelligence Applications to grow within the sector

We have already been many successful deployments of artificial intelligence (AI) applications across the hospitality industry. This technology has the potential to enormously improve customer service levels whilst providing more time for human resources to get other tasks done. This makes AI absolutely vital for the future of the sector. AI enabled facial recognition technology is another area, which is driving innovations like VIP Guest Alerts and personalised greetings, etc.

Focus on Cybersecurity

It is arguably even more important for those in the hospitality sector as this is naturally an industry that handles a large amount of customer personal details. This makes hospitality businesses are an obvious target for hackers. Hackers and cyber criminals are becoming increasingly sophisticated – this means that is necessary for companies to focus more on Cybersecurity compliance in the hospitality ecosystem.

Use of Virtual Voice Assistant Technologies

The hospitality sector has already beginning to see a huge range of uses for voice assist technology, but as its adoption grows that may be some unforeseen possibilities. Whether it is being used to check-in or get customer assistance, it may soon be possible for customers to simply speak to a mobile phone screen and get everything sorted."

As per Khemka, "Smart technology is changing everything from the homes we live in to how our cities are managed. The hospitality industry is no exception. In many ways, the hospitality industry is leading the charge in the adoption of smart business technology.

Gone are those days when hotels used to hand over metal room keys to guests and maintain a guest register to record guest information and assign rooms. Technology has been ever booming in the hospitality industry with new innovations coming up every year. Did you ever imagine your hotel would have a self-check-in kiosk? Or even a dumbwaiter facility? Quite a shift has happened from the previous hotel practices and what is followed now.

One of the main benefits of smart technology is how it aggregates data and makes it actionable. But with big data comes big responsibility. According to Khemka, 'Big data is great when you can use it to take action—whether that's tackling a new market segment or adjusting your rate plans to compete against your competitors. However, the biggest concern around big data and the

Parthesh Dhaggal
Founder,
Enceplon

> "While most cybersecurity solutions concentrate on anti-malware tools, firewall configurations, and other data security measures, however, physical security of IT resources is just as important."

necessary data harboring is the safety around it. Every data harborer's goal is to keep their customers' data safe, but that's easier said than done. In recent years, we've seen massive data breaches that have literally put hundreds of millions of consumers at risk—like Equifax and Target.'

He continues, 'As the price point of big-data solutions makes them more accessible to medium-sized segments of the hotel market, we can expect to see more hotel owners adopt and invest in them. More importantly, we can expect solution providers who can guarantee data protection to dominate their market segments.'

Mobile applications have also come up with this facet to provide convenience and choice to guests. Guests are updated when their room is ready, allowing them to bypass the front desk. Marriott.Inc introduced their mobile app, empowering guests to check-in after 4 PM, a day prior to their check-in date. Leveraging this innovation, your staff can focus on delivering a high level of service that guests are always looking for.

NFC has been here for over a decade now. But what is NFC? NFC enables seamless transmission of data from compatible devices over a short-range with the help of radio waves. It is widely used commonly for payments, sharing media files, or any other form of data by a single tap. All that's required is this little device we know as smartphones that enable NFC.

So how can NFC work for a hotel? Well, to begin with, NFC can reduce the load of work at the front desk by enabling faster check-ins and check-outs. Moreover, it provides the function of making secure payments and shields against theft or loss. As discussed earlier, digitized room keys can be shared over this technology ensuring safety and misplacement of keys.

'The leisure and hospitality industry is one of the driving forces of the global economy. The widespread adoption of new technologies in this industry over recent years has fundamentally reshaped the way in which services are provided and received. Thermal imaging and facial-recognition technologies are also being introduced to the general public through the advent in this industry only. Facial-Recognition technology is one of the most important emerging tech trends in general, but its potential uses in the hospitality industry are especially interesting. In particular, biometrics is being used to usher in a new age of seamless authentications, and this could benefit hotel processes and customer purchases', states Khemka.

For example, imagine if a fingerprint or facial recognition technology could be used in your hotel to unlock rooms. Now consider the uses of the same technology for check-in and check-out purposes. In the future, this technology is also likely to allow for completely seamless purchases, with payments being authenticated by touch.

Thermal imaging is also used to scan a large number of people quickly, which enables a broader view and the possibility of identifying those with elevated temperatures more proactively. First fielded during the 2003 SARS epidemic, thermal fever screening systems use cameras that detect the infrared energy invisible to the human eye that people and objects emit. Whether it's a medical organization, event, business, airport, or hotel that wants to implement this screening before you enter, the demand for this tech is going to be greater than ever before. Though it can be perceived as invasive, it could prove invaluable in helping us manage larger gatherings as events, conferences, and sports-oriented outings. The various CP PLUS thermal imaging solutions have been proven to be highly efficient and are becoming increasingly popular in the market."

As per Kadakia, "With the traditional demand disrupted and the abrupt demand for COVID-19 counter solutions, these industries have revamped their product portfolios. With a focus on automation and strengthening the efficiency of the hospitality sector, the solution makers are offering solutions that minimize the time invested in operating. Again, the road ahead builds the opportunity for thermal screening solutions that can coin down threats.

Likewise, in order to enable smooth management of the staff, various hoteliers have opted for contactless access control solutions. These solutions are being adopted by various hoteliers at present. As a result, a heavy emphasis on contactless solutions is likely to remain prevalent."

According to Holla, "Some of the technological advancements for security in this sector are –

- **Utilization of a strong solution that is well secured**– A strong cybersecurity solution is an absolute necessity in today's changing world when organizations were forced to opt for remote working due to the pandemic. We, at Axis Communications firmly believe that our cameras are very secured and comes with end-to-end security

- **Voice Control** – The demand for voice control is growing. This involves the use of smart audio devices like speakers located at different points in the hotel
- **Facial Recognition Technology** – Facial Recognition can be utilized for seamless operations - from checking in guests to maintaining employee attendance
- **People Counting** - Our People Counting solution has been specifically curated for measuring and taking faster action to avoid congestion or a queue and maintain social distancing norms, which is so crucial for the hospitality sector. It gives analytics and valuable insights such as – how many employees are in an area like a, cafeterias, lift lobbies, a specific floor, kitchen, or sites at the same time, how they move, where they congregate, and periods of peak occupancy. These insights further enable the management to plan accordingly and take immediate action to make social distancing normal while improving service, operational efficiency and profitability
- **AXIS Occupancy Estimator** - AXIS Occupancy Estimator offers a cost-efficient way to accurately estimate occupancy levels on the hotel site to comprehend visitor patterns better and how the space is used. It provides real-time data on how many people are present in the premises or in a certain area at a certain time. This valuable data helps in increasing operational efficiency to maintain the premises and avoid crowding, optimize workforce planning and opening hours and take necessary measures to adhere to the social distancing guidelines
- We have collaborated with **Application Development Partners** (ADP) to provide solutions such as Social Distancing solutions, Touch Free solutions, Body Temperature Monitoring solutions, Mask Detection solutions and Touch Free Attendance systems with facial recognition capabilities to offer top-notch solutions to create a secure working environment for all employees and customers
- **Audio solutions and Public Announcement** solutions are becoming important too, in the current context of the pandemic, to better manage and monitor employees and guests so that they follow and adhere to the social distancing norms better"

As per Dhaggal, "The hospitality industry has come a long way. The technological advancements in this sector are mind boggling. They include Contactless checkins and check outs, Wi-Fi infrastructure overhauls, digital conference facilities, mobile communication and automation, NFC technology, Robots and infrared sensors, smart room keys, entertainment on tap, cloud services, contactless payments, mobile check ins, facial Recognition Technologies, automated check in and checkout, digitized room keys.

Another technological trend within hospitality management is the 'Internet of Things', or IoT, involves extending internet connectivity to everyday objects, devices and appliances. These devices can then collect data and communicate or interact over the internet, turning previously unintelligent devices into 'smart' devices, which are often semi or fully autonomous.

Internet - enabled thermostats, which are used to automatically adjust room temperatures at check-in and check-out times, or in response to temperature swings caused by the sun, or by windows being opened. The same concept is also being deployed for lighting, improving energy efficiency by, for instance, reducing light intensity during daylight hours.

Artificial Intelligence - In the modern age, customers expect to be able to interact with hospitality companies across a variety of digital channels and receive rapid responses. Of course, actually having staff monitoring all of those channels and delivering swift responses can be difficult, if not impossible, which is where chatbots artificial intelligence (AI) come in.

Chatbots are able to understand simple questions and provide answers almost instantaneously, taking the burden away from customer service staff and improving the experience for customers. Meanwhile, AI's uses extend into other important areas for hotels too, including data analysis.

Virtual reality is another of the major technology trends in the hospitality industry.