Cybersecurity in Hospitality: Protection Guaranteed!

Cybersecurity plays a pivotal role in safeguarding the hospitality industry as it protects guest information, upholds trust, and sustains business performance.

BY BINDU GOPAL RAO

Pravin Pandey, Multi Property IT Manager – Mumbai North IT Cluster, The Westin Mumbai Garden City

Suman Sur, Director and Head of Information Technology, THE Park Hotels

Vinesh Gupta, General Manager, The Den

Threats like ransomware attacks, phishing attacks, distributed denial-of-service (DDoS) attacks, and human error mean that hotels need to ensure that their customer data is safe.

HOSPITALITY CONNECT

The role of cybersecurity in the hospitality industry is very important and critical due to the sensitive nature of customer data and the potential impact of cyber threats on hotel operations and reputation. "Cybersecurity ensures the protection of guests' personal information, such as credit card details, passport information, and booking preferences, from unauthorized access, theft, or misuse. It also safeguards the integrity of the hotel's systems and infrastructure, preventing disruptions to services and maintaining guest trust which is very important," says Pravin Pandey, Multi Property IT Manager – Mumbai North IT Cluster, The Westin Mumbai Garden City.

POST PANDEMIC RECOVERY

Since the pandemic hit the hospitality industry hard, it has made significant steps toward recovery. Hospitality must remain vigilant to continue this recovery amid an evolving cyber threat landscape. "With new-gen cyber threats increasing in frequency and sophistication, we at THE Park Hotels take cognizance of every touch point and take steps to protect data with robust IT security policies and procedures. Data is the new oil and so collecting, processing, and storing large amounts of customer data makes the hospitality business attractive to cybercriminals. Cybercriminals can misuse guest infor-

> *"Hackers are constantly looking for new ways to penetrate security systems and that's why it is important for hotels to invest in robust cybersecurity solutions."*
>
> **Vinesh Gupta**

mation on the dark web, hackers can use stolen data to create realistic communications with unsuspecting customers. With stolen personal data, criminals can develop and distribute fake confirmations, updates on non-existent loyalty programs, and bogus transfer requests, intending to trick guests into sharing more data or performing financial transactions. Card readers, POS systems, IoT devices, Wi-Fi and hotel websites are a few top vulnerabilities for the hotel industry and operators need to be more vigilant on these critical assets," says Suman Sur, Director and Head of Information Technology, THE Park Hotels.

STAYING SAFE

The hospitality industry, like all other industries, has undergone radical changes due to rapid technological advances. India's rapidly growing Gen Z and Gen Alpha has led to an increase in cyber threats to hotels. As a treasure trove of sensitive guest information, the hospitality industry has become an attractive target for cybercriminals exploiting vulnerabilities. "The dynamic nature of cyber threats presents a significant challenge for the industry to initiate cyber security initiatives. Hackers are constantly looking for new ways to penetrate security systems and gain access to important visitor information and that's why it is important for hotels to constantly update their defences and invest in robust cybersecurity solutions," says Vinesh Gupta, General Manager, The Den.

SECURE MEASURES

To protect sensitive data and minimize cyber threats, cybersecurity measures are essential. Also, cybersecurity is an ongoing effort, and staying vigilant is essential to protect against cyber-attacks. Ashish Bhawsar, IT Manager, The Ritz-Carlton Pune, says, "Always encrypt your enterprise endpoints and data. Conduct continuous cybersecurity training for staff to maintain a well-prepared workforce. Educate them on identifying suspicious behaviour and reporting it promptly. To find vulnerabilities and fix them early, invest in penetration testing on a regular basis. Ensure that there is a strong enterprise password policy to prevent unauthorized access. Keep software and system updated to patch security vulnerabilities." Vishal Singh, General Manager, JW Marriott Chandigarh ,adds, "All systems require unique identification for access, and for compliance reasons, no employee can share their ID with another. Failure to provide this unique ID will result in the inability to access the systems. Additionally, it is crucial to regularly change passwords to prevent potential access issues."

Ashish Bhawsar, IT Manager, The Ritz-Carlton Pune

Vishal Singh, General Manager, JW Marriott Chandigarh

Krishnanand Bhatt, Director, Technology Advisory, Nexdigm

> *"Always encrypt your enterprise endpoints and data. Conduct continuous cybersecurity training for staff to maintain a well-prepared workforce."*
>
> **Ashish Bhawsar**

BREACH BARRIER

When breaches occur in the hospitality industry, they are managed through immediate containment, investigation, and notification to affected parties. Common breaches include data theft, ransomware attacks, and phishing scams. "Hotels deploy incident response teams, conduct forensic analysis, and reinforce security measures. Regular training, backups, and collaboration with cybersecurity experts help mitigate and prevent such incidents, ensuring guest data and operations remain secure. Additionally, advanced cybersecurity measures, cloud computing, IoT devices, AI for personalized services, and contactless payment systems are widely utilized. These technologies enhance guest experiences, streamline operations, and improve security," says Krishnanand Bhatt, Director, Technology Advisory, Nexdigm.

Pankit Desai, Co-Founder & CEO, Sequretek, adds, "Despite investments in people, process and technology, breaches do occur. It is important for organisations to prepare for post-breach scenarios, to ensure that there is a minimum hit to business continuity. A well-defined incident response and recovery plan needs to be in place, and the plan needs to be tested out periodically to make sure that it will work seamlessly in the event of an actual breach."

TECH TALK

Cybersecurity in the hospitality industry is witnessing a transformation with advancements in AI, large language models (LLMs), and natural language processing (NLP). AI-driven predictive analytics can detect potential threats before they occur, and automate real-time threat detection and response, minimizing operational disruptions. "NLP analyses internal communications to detect anomalies and efficiently manage incident reports through virtual assistance. Machine learning algorithms continuously adapt to new threats, while blockchain ensures data integrity and security. AI and ML create sophisticated guest profiles for personalised services without compromising security and monitor IoT devices to detect anomalies," says Kumar Ritesh, Founder & CEO, Cyfirma.

> *"It is important to set up firewall devices properly and check them regularly to ensure their software/ firmware is up to date."*
>
> **Murlidhar Rao**

Pankit Desai, Co-Founder & CEO, Sequretek

Kumar Ritesh, Founder & CEO, Cyfirma

Murthy Kolluru, IT Manager, Novotel & Ibis Bengaluru Outer Ring Road

Murlidhar Rao, Chief Operating Officer, Araiya Hotels and Resorts

SECURITY MATTERS

Beyond technological measures, fostering a culture of cybersecurity awareness among employees and guests is essential. "Hotels employ various measures to bolster cybersecurity, including robust firewalls, encryption protocols for data transmission, network segmentation to limit access to sensitive information, regular security audits and penetration testing, employee training on cybersecurity best practices, and the implementation of strict access controls to prevent unauthorized access to critical systems," says Murthy Kolluru, IT Manager, Novotel & Ibis Bengaluru Outer Ring Road. Murlidhar Rao, Chief Operating Officer, Araiya Hotels and Resorts, adds, "Firewalls act as a barrier to prevent the spread of cyber threats such as viruses and malware. It is important to set up firewall devices properly and check them regularly to ensure their software/ firmware is up to date. Implementing strong password policies and using multi-factor authentication (MFA) can enhance information security controls. Tougher passwords amplified with MFA should be used in every device to ensure data security."

Adopting a proactive approach to cybersecurity, coupled with a strong culture of security awareness and compliance, strengthens the resilience of hotels against cyber-attacks and instils confidence among guests in the protection of their data. H