Shiji

Hotel Cybersecurity in 2024:

The latest threats and best practices for keeping guest data secure

Content

Shiji Group

Shiji

01

Cybersecurity:

A company-wide responsibility

On a quiet night on Christmas Eve, a Vancouver hotel's computer network ground to a halt. Shortly after, an anonymous message came in from a group of hackers demanding that the hotel pay $125,000 immediately or its systems would be disabled permanently.

"Suddenly, it was chaos," the general manager told Shiji recently. For the small, regional hotel company, it was the start of a nightmare that would take months to recover from and would act as an impetus to migrate to a modern cloud-based PMS platform.

Today, similar scenarios are playing out around the world as the hotel industry grapples with an alarming uptick in data breaches, malicious viruses, and ransomware attacks. A breach can have a devastating effect on a hotel, disrupting operations, undermining guest trust, and requiring enormous outputs of time and money to resolve.

This whitepaper explores the evolving landscape of cybersecurity, including the latest threats, technological advances, and best practices, as well as the growing need to broaden responsibility for safeguarding guest data from the IT department to the entire organisation

A breach can have a devastating effect on a hotel, disrupting operations, undermining guest trust, and requiring enormous outputs of time and money to resolve.

02

Rising threats in hotel cybersecurity

In fact, almost **one-third** of hospitality organisations have reported a data breach in recent years, with an average cost of about US$3.4 million, according to Trustwave. [1]

2023 witnessed a wave of data breaches, underscoring the escalating threat landscape. Within one month in the fall alone, three incidents shook the hospitality industry:

- A cyberattack at MGM Resorts International in Las Vegas disabled the company's systems for two weeks, incurring estimated l**osses of $100 million.**
- After an attack that compromised data related to its guest loyalty program, Reno-based Caesars Entertainment reportedly succumbed to a **ransom demand of $15 million.**
- A breach at Munich-based Motel One Group resulted in the **theft of almost 25 million files**, including guest booking confirmations from the previous three years.

[1] *Cybermagazine. Trustwave report on hospitality industry security threats. September 2023.*

Cyberattacks are nothing new to the hospitality industry. Over the past several years, the world's biggest hotel brands have experienced breaches, including Hilton Hotels & Resorts, InterContinental Hotels Group, and Wyndham Hotels & Resorts. In 2018, a breach at Marriott International affected as many as 500 million guest records, costing the company an estimated $500 million. Despite the best efforts made by these companies to protect systems and data, cybercriminals still found a way to hack into their systems, underscoring the vulnerability of all types of hotel companies.

Today, what is new are the targets. **"The recent breaches weren't at the usual top hotel chains, they were niche, mid-sized hotel companies,"** said Michael Heinze, Chief Architect at Shiji. "Data security has become a top priority for all types of hotel companies. Everyone wants to know how they can prevent the same thing from happening to them."

"Nowadays, ransomware is the number one threat to hospitality businesses, Bad actors want to hack into a company's network, gain access to sensitive resources, encrypt and copy data from servers. Then they demand a ransom for the decryption key, but also threaten to publish data publicly, sell it, or use it for other criminal purposes if the hotel doesn't pay" said Aleksander Ludynia, Chief Security Officer at Shiji.

"Bad actors want to hack into a company's network, gain access to sensitive resources, encrypt and copy data from servers."

- Aleksander Ludynia
Chief Security Officer at Shiji

The latest tactics used by cybercriminals

Motives behind cyberattacks can vary, encompassing external threat actors such as hackers, criminal groups, government entities, competitors, or even insiders like current and former employees and contractors. The primary motivation, however, is often financial gain. Personal data and payment information are highly valuable to cybercriminals, who can use it to hack into bank accounts, sell it to third parties, and leverage it to blackmail companies.

Hackers draw on a growing array of tactics to gain access to this data, often recruiting unwitting employees. According to Verizon, **74 percent of breaches involve the human element[2].**

Common tactics include:

- **Social engineering attacks:** Manipulating individuals to divulge confidential information.
- **Phishing scams:** Deceptive emails from seemingly genuine sources to extract sensitive information.
- **Brute-force attacks:** Utilising automated bots to guess passwords through trial and error.
- **Denial-of-service attacks:** Disrupting operations by disabling user access to computers or networks.
- **Malware:** Installing harmful software, including viruses, worms, and ransomware.

In recent years, cyberattacks have become more sophisticated, often coordinated by organised criminals who operate like a business. In the travel industry, for example, the DarkHotel group targets business travellers through hotel Wi-Fi networks. Other groups sell "ransomware as a service" on the dark web, offering software kits containing hacking tools and code, tech support, and even user reviews in exchange for a cut of the profits[3].

[2] Verizon. 2023 Data Breach Investigations Report.
[3] Barron's. How Ransomware Gangs Are Fueling a New Cybersecurity Arms Race.

Risks to hotels and their guests

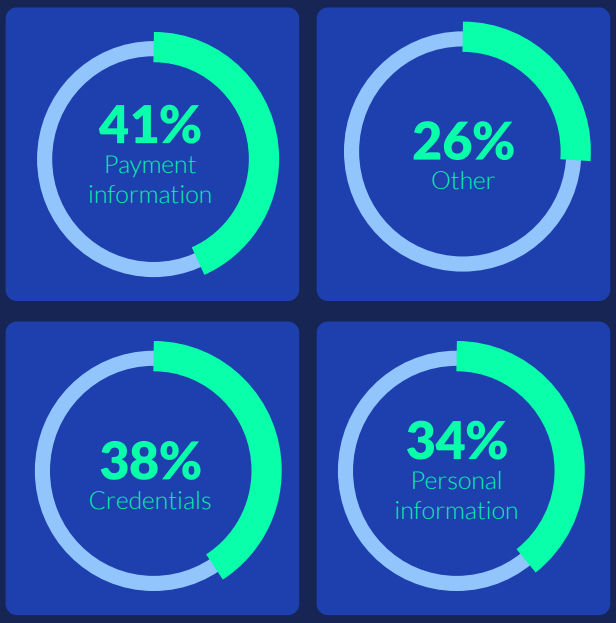
When threat actors gain unauthorised access to guest data, guests are exposed to identity theft, financial fraud, and other malicious activities. Hotels face disruptions to operations, revenue losses, legal action, and government penalties. Disclosure of breaches, now required by law in some jurisdictions, can lead to bad publicity, a drop in share value, erosion of consumer trust, and damage to reputation.

When it comes to ransomware attacks, hotel owners are forced to make a tough decision: pay the ransom or face dire consequences. In 2023, ransomware hacks cost organisations an estimated $30 billion. **The costs can be up to 10 times the amounts paid in ransom, averaging $4.5 million per incident,** in addition to legal fees, system upgrades, and regulatory fines[4]. A survey from Splunk found that 83% of organisations paid ransoms following a ransomware attack, with more than half paying at least $100,000[5].

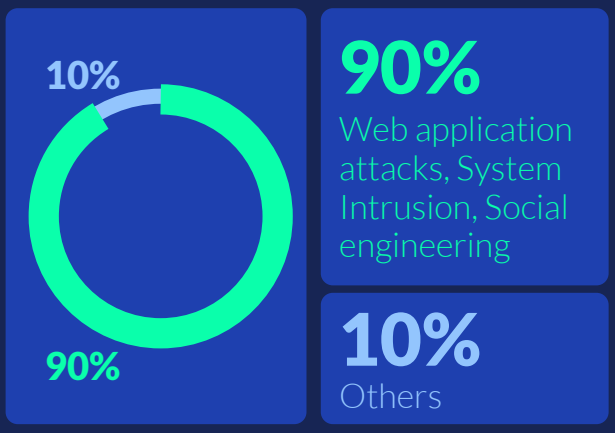
What breaches are most common in hospitality?

Verizon's 2023 Data Breach Investigations Report analysed 254 data security incidents in the accommodation and food services sector, revealing key insights:

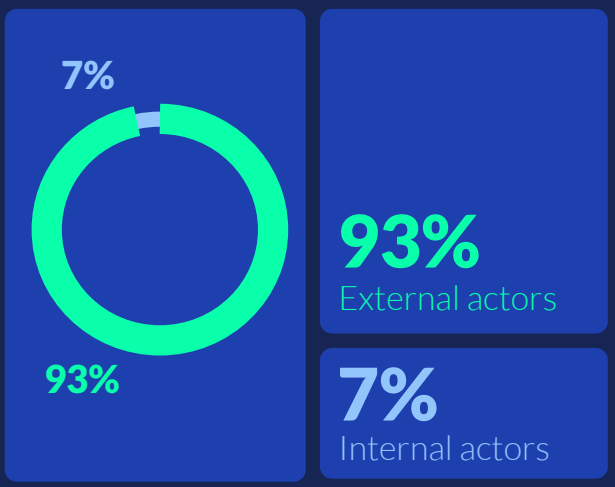
Type of compromised data



Breach methods



External vs. Internal actors involved in breaches



[4] *Ibid*
[5] *Splunk. CISO Research Reveals 90% of Organizations Suffered At Least One Major Cyber Attack in the Last Year; 83% Report Ransomware Payments, October 2023.*
[6] *Verizon. 2023 Data Breach Investigations Report.*

03

Balancing personalisation with data protection

Given the risks, cybersecurity has ascended to the forefront of priorities for hospitality businesses, necessitating a collective effort from the brand level to property levels. The focus revolves around two crucial objectives:

- **Data privacy:** Ensuring guest personal information is collected, stored, and used responsibly to protect their privacy.
- **Data security:** Safeguarding computer systems and data from unauthorised access, theft, and malicious attacks.

"Hotel companies are typically direct targets for attackers, but this year witnessed instances where they became just one layer in multi-step phishing campaigns". "Fraudsters are targeting travellers by exploiting vulnerabilities in hotel systems, and are subsequently abusing the communication platforms associated with these systems to send fraudulent payment requests to unsuspecting customers" said Bart Hessels, Team Lead Offensive Security, Adyen.

"Fraudsters are targeting travellers by exploiting vulnerabilities in hotel systems."

- Bart Hessels
Team Lead Offensive Security, Adyen

Hotels:
A prime target for cybercriminals

No one understands daily operational challenges better than frontline employees. By soliciting their input about pain points and needs, hoteliers can ensure technology solves real-world problems, perhaps in ways that would not otherwise have been considered.

Growing tech dependence

Over the past few years, hotel companies have adopted technology at an unprecedented rate. Today, hotels use dozens of applications that store and share guest data, amplifying exposure.

Abundance of sensitive information

Hotels amass volumes of sensitive data, including guest contact details, identification, credit card information, and personal details like gender, nationality, employer, and birthdates. Some of this data is retained for years.

Access needs

Guest data must be accessible to hotels throughout the customer journey, from time of reservation to post-stay, to enable core functions like customer relationship management (CRM), personalising the guest experience, and building guest loyalty. Every touchpoint exposes data to potential breaches.

Flow of guests

With 24/7 operations and a constant flow of guests arriving from all over the world, hotels become a prime target for hackers seeking vulnerabilities.

Employee turnover

Managing cybersecurity training and awareness for teams across various departments, properties, and locations is challenging, especially given high turnover and the number of part-time and contracted employees.

Complex business models

The intricate structure of hotels, often involving property ownership, franchising, and management by different entities, complicates the division and oversight of cybersecurity responsibilities.

Elevated expectations

Travellers now demand heightened data protection, with new regulations and recent breaches making it all the more challenging for hotels to strike a balance between personalization and privacy protection.

Phishing for payments

Recently, there has been a spate of incidents at hotels around the world involving hackers posing as former guests to trick hotel staff into downloading malware. The malware provides access to the hotel's computer network, which is then used to gain unauthorised access to the hotel's Booking.com account. Subsequently, hackers solicit payments directly from guests with upcoming reservations. The incidents showcase the increasingly audacious behaviour of cybercriminals in the travel industry.[7]

[7] BBC, *Booking.com hackers increase attacks on customers*. November 2023.

04

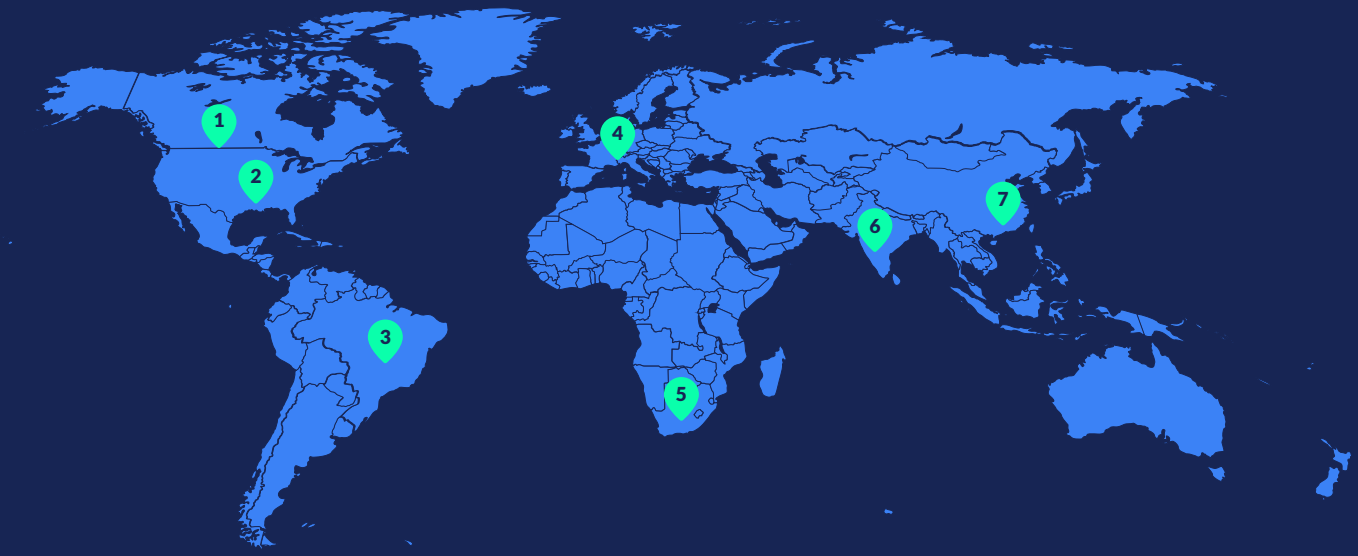
Governments cracking down:

Evolving privacy regulations

Navigating the intricate and evolving web of privacy laws and regulations poses a significant challenge for hotel companies today. To date, 80% of countries have enacted cybercrime legislation, according to UNCTAD. [8]

A snapshot of key regulations related to data security and privacy includes:

1. **Canada:** Personal Information Protection and Electronic Documents Act (PIPEDA)
2. **United States:** Various federal and state laws
3. **Brazil:** General Data Protection Law (LGPD)
4. **Europe:** General Data Protection Regulation (GDPR)
5. **South Africa:** Protection of Personal Information Act (POPIA)
6. **India:** Digital Personal Data Protection (DPDP) Act
7. **China:** Personal Information Protection Law (PIPL)



[8] *United Nations Conference on Trade and Development (UNCTAD). Cybercrime Legislation Worldwide.*

Shiji

The GDPR, introduced by the European Union in 2018, set strict new standards for consumer privacy protection in Europe while also influencing regulations globally.

Despite providing some clarity to consumers and businesses, privacy laws have become increasingly difficult to interpret for hotel companies, particularly those operating in multiple countries.

Intricacies of data sovereignty laws

According to the concept of data sovereignty, data is subject to the laws and regulations of the country where it is collected, processed, and stored. Ultimately, these laws are designed to protect citizens as well as national security. For global hotel brands, however, determining which laws apply to what data is not always easy. Data is often collected in one country, stored in another country, and used in another country. Things become even more complicated when data is transferred from one country to another.

In countries such as the United States and China, the government maintains the legal right to access any data stored on its soil. To assert control over data and ensure compliance with regulations, some governments have introduced localization laws, or data residency laws, which require organisations to keep certain types of data within the country's borders. In China, for example, Western companies have been fined for transporting the personal data of Chinese citizens out of the country.

In Europe, the GDPR authorises organisations to collect and process the personal data required to perform their core services. While permission for cross-border data transfers within an international organisation is not required, hotels are required to inform guests what will happen to their personal data, including where it may be transferred and why, and to make assurances it will be protected wherever it goes.

Expect more regulations to come

This is just a sampling of the intricacies of international regulations, and things are destined to become more complex over time. In the U.S., for example, the Securities and Exchange Commission (SEC) now requires publicly traded companies to report material breaches within four days. In Australia, the government can now issue fines of up to AUD $50 million for non-compliance. As the legal and regulatory landscape evolves, hoteliers will be further challenged to keep up with changes and maintain compliance.

"Hotels and technology providers should approach data sovereignty as a moving target. Most countries are working on new, stricter privacy regulations, and data sovereignty is an integral part of these regulations. Picking your vendors based on their compliance to data sovereignty laws is crucial to prevent your valuable customers' information from getting into the wrong hands", said Michael Heinze, Chief Architect at Shiji.

"Picking your vendors based on their compliance to data sovereignty laws is crucial to prevent your valuable customers' information from getting into the wrong hands."

– Michael Heinze,
Chief Architect, Shiji

05

More technology, more vulnerabilities

Recent technological advancements in the hotel industry have undoubtedly increased operational efficiency and improved the guest experience. However, the progress comes at a cost, elevating the vulnerability of hotels to cyberattacks and data breaches.

“Hotels must acknowledge the risks associated with incorporating new technology into operations, even though cybersecurity isn’t inherently their core responsibility,” warns Ludynia of Shij.

Report after report, study after study shows that many attacks are successful because network owners did not know their enterprise assets, the software they had running, and where their critical data was.

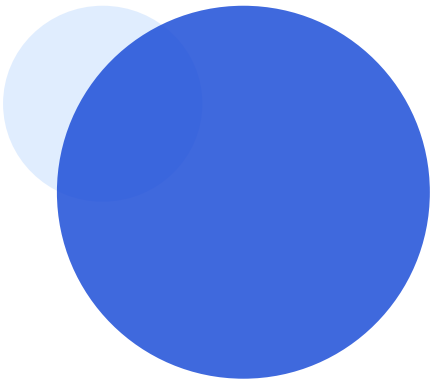
Knowing your environment is foundational to any cybersecurity program … After all, you can’t protect what you don’t know you have.” – Center for Internet Security.[9]

The weakest link: legacy systems

Major hotel data breaches often stem from hackers gaining access to guest profile information stored in outdated PMS and point of sale (POS) systems. Legacy systems struggle to adapt to modern cybersecurity threats and comply with privacy regulations.

In contrast, **contemporary PMS and POS platforms offer built-in privacy and security features, such as GDPR-compliant anonymisation of personal information.** Moreover, some newer platforms are built on microservice architecture, providing an added layer of security by housing applications and data in independent zones.

[9] Verizon. 2023 Data Breach Investigations Report.



Migration to the cloud: risks and benefits

The trend of migrating computer systems to the cloud for increased operational efficiency, scalability, and cost reduction brings both advantages and risks. While centralised data management enhances security, concerns around cloud security rank high in a PwC survey, with 47% of business and tech executives identifying it as their top cyber risk concern.[10]

Choosing a cloud service provider with robust security protocols becomes paramount to mitigate risks effectively. Global providers operate data centres around the world, enabling hotel companies to choose where to store data and whether to replicate it to other regions.

The lure of payment data

Handling payment information remains a highly vulnerable aspect for hotels. The proliferation of online reservations, varied payment methods, and card-not-present transactions intensifies the challenge. A recent breach at Hilton was found to have originated from malware in POS systems at restaurants and shops, allowing hackers to access guest credit cardholder numbers, security codes, and expiration dates.

Such vulnerabilities underscore the importance of collaborative efforts among payment tech providers, hotels, and third-party vendors. The **implementation of end-to-end encryption, tokenization, and fraud detection tools**, along with ensuring PCI DSS compliance have become standard defence protocols.

Self-service applications: not just convenient for guests

The demand for self-service options has surged in hotels in recent years, driven in part by the pandemic. While applications such as mobile check-in, keyless room entry, and digital food ordering provide enhanced guest convenience, they also introduce potential vulnerabilities. Granting guest access to hotel systems through such applications provides cybercriminals with additional exploitable entry points.

Internet of things: extending the attack surface not just convenient for guests

The proliferation of internet of things (IoT) applications in hotels, including self-serve kiosks, security cameras, temperature and lighting controls, smart minibars, and voice-activated assistants, enhances efficiency and the guest experience but simultaneously extends the potential attack surface. Meanwhile, more employees are working from home, using personal computers, smartphones, and Wi-Fi networks to connect to hotel systems.

Hotel Wi-Fi networks often serve as entry points for data breaches, emphasising the need for robust security measures. If one device is compromised, all connected applications and devices are at risk too. In one infamous incident, hackers broke into the network of a North American casino through an internet-connected device tank that regulated the temperature, food, and cleanliness of a fish tank.[11]

[10] *PwC. The C-suite playbook: Putting security at the epicenter of innovation. October 2023.*
[11] *The Washington Post. How a fish tank helped hack a casino. July 2017.*

06

Nine best practices in hotel cybersecurity

Careful vetting and selection of technology partners now represents an essential criterion of cybersecurity practices.

After the Vancouver hotel was hacked, the hotel's owners refused to pay the ransom. Instead, the company's IT department rebuilt the network from scratch. It was a lengthy, costly process that required staff to work around the clock and tested the patience of guests at times. The team wondered, what could they have done to prevent this?

Investing in preventative measures has proven to be far more cost-effective for organisations than dealing with the aftermath of a breach. Here are eight proactive measures for hospitality companies to consider.

1) Practice basic security hygiene

According to Microsoft's Digital Defense Report 2023, 99% of cyberattacks can be prevented by following these five practices[12]:

- ✓ Enable multi-factor authentication (MFA)
- ✓ Apply "Zero Trust" principles
- ✓ Use extended detection and response (XDR) tools and antimalware
- ✓ Keep systems up to date
- ✓ Protect data

Additional precautions for hotels include:

- ✓ Use strong passwords and keep them private in password manager
- ✓ Implement a unique password per application
- ✓ Lock computers when leaving workstations
- ✓ Store and process only necessary personal data
- ✓ Separate guest networks from hotel networks and protect them
- ✓ Maintain backups of systems, data, and reports
- ✓ Manage vulnerabilities

2) Maintain a comprehensive, dynamic cybersecurity policy

At the core of a hotel company's security strategy is its cybersecurity policy. This document delineates policies and procedures governing the collection, storage, and usage of guest data. It also outlines roles, responsibilities, communication channels, and expectations, distributing responsibilities among ownership, corporate office, property staff, contractors, suppliers, and partners.

The policy functions as a live document that evolves over time, serving as a guideline for decision-making and a reference point in the event of a breach. As part of its maintenance, Ludynia of Shiji stresses the importance of establishing and periodically enhancing incident management processes to prepare for potential attacks.

3) Use a cybersecurity framework

In addition to the GDPR, organisations often leverage the one of the many available security models and frameworks to shape their security policies:

- ✓ CIA Triad. A model guiding the development and implementation of security systems, emphasising confidentiality (ensuring data privacy), integrity (safeguarding data accuracy and reliability), and availability (ensuring timely access to data and services).
- ✓ ISO/IEC 27001 Family. An international standards for information security management systems (ISMS) defining requirements and providing guidance.
- ✓ NIST Cybersecurity Framework. A voluntary set of guidelines, standards, and best practices for cybersecurity risk management, offering a structured approach to identifying, protecting, detecting, responding to, and recovering from cybersecurity events. NIST also offers a special publication for securing hotel PMSs. [13]

[12] *Microsoft Digital Defense Report 2023. October 2023.*
[13] *NIST. Securing Property Management Systems. March 2021.*

4) Select the right technology partners

Careful vetting and selection of technology partners now represents an essential criterion of cybersecurity practices. This involves reviewing security and privacy standards and ensuring compliance with regulations, company policies, and industry best practices (including ISO/IEC 27001, ISO/IEC 27018, and PCI DSS standards). Partners should maintain a dedicated team of certified security experts, continuously monitor systems, and collaborate exclusively with trusted third-party suppliers.

5) Take a least privileged access approach

To fortify systems against intentional breaches or those resulting from employee negligence, hotel companies should meticulously manage access levels for each department and role. Experts advocate for a "least privilege access" approach, restricting users and systems to the minimum access necessary for their duties.

6) Make payments more secure

"Hotels are more exposed to fraudsters and risk than other industries given the complexity of the guest journey," said Mark Rademaker, VP Hospitality at Adyen. "Hoteliers need to remain vigilant and understand not only how payments are being transacted via their direct channel, but also via their OTA partners. Equally important is understanding their partner ecosystem. For example, a decision by the PMS provider might cause a hotel to be in PCI scope."

Rademaker recommended three ways hotels can make payments more secure:

- ✓ Remove any visible exposure to raw card data. "Europe seems to be in a better place, but we still see hotels in North America and Asia accepting raw card data on forms or via guest phone calls," he said.
- ✓ Add tokens above property whenever possible. Tokenization is table stakes at this point and should be a standard offering for all hotels.
- ✓ Improve management of e-commerce transactions through the use of risk tools (i.e. white lists, machine learning risk rules, 3DS, A/B testing).

7) Monitor systems

Continuous system monitoring and vigilance against suspicious activity empower hotels to prevent breaches and respond swiftly to successful attacks. Combining tools like firewalls, antimalware, and XDR, along with regular penetration testing to uncover vulnerabilities, helps to ensure a robust defence. While larger companies may maintain an in-house cybersecurity team, smaller ones might consider outsourcing responsibilities to a managed security service provider.

8) Assess risk

Risk assessment encompasses regular audits of systems and procedures to comprehend the company's risk profile. This includes reviewing how applications share information such as reservations, guest profile information, and payments, and scrutinising staff knowledge levels and adherence to security protocols. By assessing risk levels and potential impacts, hospitality organisations can allocate resources to areas with the highest risk.

9) Continuously instil cybersecurity awareness

Staff awareness of cybersecurity threats and protocols is crucial. Cybersecurity must become everyone's concern, not just the IT department's. Employees, who are often primary targets, must act as the first line of defence. Continuous education, training on risks, responsibilities, and procedures, frequent updates about the latest threats and tactics, and constant vigilance are essential components of a comprehensive cybersecurity strategy.

Cybersecurity: **A Top Budget Priority in 2024**

In 2024, global spending on security and risk management is projected to reach $215 billion, marking an increase of 14.3% over 2023, according to Gartner, Inc. "The continuous adoption of cloud, continuous hybrid workforce, rapid emergence and use of generative AI (GenAI), and the evolving regulatory environment are forcing security and risk management (SRM) leaders to enhance their security and risk management spending," said Shailendra Upadhyay, Senior Research Principal.[14]

[12] *Gartner. Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024. September 2023.*

07

Balancing growth with innovation in cybersecurity at Corinthia Hotel Group

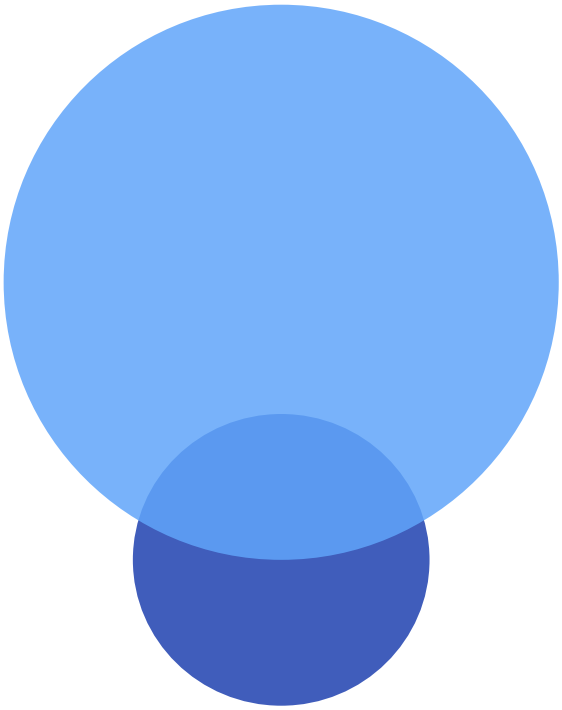
With a new lifestyle brand, Verdi Hotels, launching this year, Corinthia Hotel Group is on a sharp growth trajectory. As an integral part of its growth strategy, the iconic hotel group is commiteed to innovative technology and data protection.

"Today, hotels use more technology throughout the customer journey," Jonathon Liu, Chief Commercial Officer, told Shiji recently. "We're handling more data to personalise the guest experience, and guests are sharing more financial details online. That brings both external and internal threats to data privacy and security."

Protecting guest data requires forethought and vigilance. "The pace of change in the tech space is incredible," he said. "We may be on top of things today, but what new threats are coming tomorrow? And how can we prepare?"

"Part of the challenge is educating guests that it's more secure to share personal information and process payments online than in person."

One of the biggest challenges is the splintering of regulations and laws around the world, Liu said. “Corinthia Hotel group will operate in multiple countries and regions, and the majority of our business will be international. Keeping on top of changes to regulations and ensuring we are always as secure and compliant as possible won’t be easy.”



As part of plans to digitalise the customer journey and ensure compliance with regulations, the company is developing a customised technology stack. “We want to ensure it’s as robust and secure as possible,” he said. Part of the strategy encompasses integrating tokenization processes into hotel operations – substituting sensitive data with a non-sensitive equivalent, or token.

“Credit card tokenization is common today, but we’re taking things a step further by tokenizing customer identification too,” he said. Rather than ask guests for a credit card and passport at check-in, the company collects the information in advance of arrival, verifies and tokenizes it, and stores it centrally in a secure, cloud-based environment.

“Part of the challenge is educating guests that it’s more secure to share personal information and process payments online than in person,” Liu said. “The process requires two-factor authorisation, is secure and tokenized, and payment information stays within the system, limiting the number of people who can access it.”

Liu anticipates that this approach will soon become the standard for handling registration and payments in hotels. “When the details are managed in advance, the team has more time to spend with guests,” he said. “We can concentrate on delivering a wonderful stay.”

08

Navigating the threat landscape of the future

As more hotels retire legacy systems, invest in technology with built-in privacy and security features, and cultivate awareness, expertise, and vigilance among staff, the threat of cyberattacks will shrink, and cybercriminals will turn their attention to easier targets outside the hospitality industry.

A mere two months after the attack on MGM Resorts, a joint effort by U.S. and European law enforcement agencies yielded a decryption tool that frees computer systems from the malware used in the breach. However, this success is likely to be short-lived, as perpetrators will invariably devise new weapons.

In the evolving landscape, hotels must brace for cyberattacks that will escalate in sophistication, speed, and frequency. Future methodologies will be powered by automation and artificial intelligence, introducing new challenges such as personalised content and deepfakes that are harder to detect.

Simultaneously, however, the technology arsenal used to fight cybercrime will also witness a surge in sophistication, driven by advancements in AI and machine learning. Additionally, more countries will tighten regulations, aiming to better safeguard consumers and provide clearer guidelines for businesses.

Hoteliers can find lessons to learn and reasons for optimism in other safety and security issues. Decades ago, fires were a major threat to hotels and their guests, sometimes with devastating consequences. Today, thanks to advanced fire prevention and protection systems, strict safety protocols, and vigilance on the part of staff, major hotel fires are a rarity.

Similarly, as more hotels retire legacy systems, invest in technology with built-in privacy and security features, and cultivate awareness, expertise, and vigilance among staff, the threat of cyberattacks will shrink, and cybercriminals will turn their attention to easier targets outside the hospitality industry.

"As AI becomes increasingly accessible, organisations will adopt a dual perspective: **harnessing AI for defence while simultaneously remaining vigilant about potential threats driven by AI."**

– David Dunn, Head of Cybersecurity, EMEA & APAC, FTI Consulting[15]

[15] *FTI Consulting. 10 Global Cybersecurity Predictions for 2024. December 2023.*

About Shiji Group

Shiji Group is a multinational technology company that provides software solutions and services for enterprise companies in the hospitality, food service, retail, and entertainment industries, ranging from hospitality technology platform, hotel management solutions, food and beverage, and retail systems, payment gateways, data management, online distribution and more. Founded in 1998 as a network solutions provider for hotels, Shiji Group today comprises over 5,000 employees in 80+ subsidiaries and brands in over 23 countries, serving more than 91,000 hotels, 200,000 restaurants, and 600,000 retail outlets.

CONTACT US

ASIA PACIFIC
sales-ap@shijigroup.com
Tel: +65 62407400

EUROPE, AFRICA
sales-eu@shijigroup.com
Tel: +49 8941207171

MIDDLE EAST
sales-me@shijigroup.com
Tel: +971 45786947

UNITED STATES
sales-us@shijigroup.com
Tel: +1 4049484001

CANADA
sales-can.list@shijigroup.com

LATAM
sales-latam@shijigroup.com

GREATER CHINA
sales@shijigroup.com
Tel: +86 10593253882

Follow us!

facebook.com/shijigroup

twitter.com/shijigroup

linkedin.com/company/shijigroup

www.shijigroup.com