DISTINGUISHED.
PROGRAMS

THE UNWELCOME GUEST:

Cyber Threats in the Hospitality Sector

With the treasure trove of personal data the hospitality industry has in its possession, cyber security has become one of the biggest risks for hotels and restaurants. In fact, PwC's "Hotels Outlook Report 2018-2022" cites the hospitality industry as having the second-largest number of cyber security breaches after the retail sector, with customers' personal information being stolen and often sold on the dark web criminal black market.

In this white paper, we take a look at what makes hotels and restaurants so attractive to cyber criminals and the various types of cyber threats the industry faces. We also provide claims examples; discuss the short- and long-term impact of a cyber attack; and go over cyber security measures that should be employed, including the need for a robust Cyber insurance and risk management program.

Tackling Cyber Risks in Hospitality

Nearly all of the hospitality industry's major players have reported data breaches in the last several years – from Marriott Starwood Hotels to Hilton Worldwide Holdings, InterContinental Hotels Group, and Hyatt Hotels. Equally hit by cyber attacks is the restaurant sector including well-publicized breaches at Applebee's, Panera, Chipotle, Sonic, and Wendy's, among others.

Although these high-profile brands make headline news in the wake of a breach, small establishments are also vulnerable. According to Verizon's 2019 Breach Investigation Report, 43% of cyber attacks are aimed at small businesses with digital incidents now costing firms of all sizes $200,000 on average and 60% closing their doors within six months of being victimized. Within the hospitality industry, Verizon says about 86% of breaches occurred at small businesses.

43%

of cyber attacks are aimed at **small businesses**

$200K

average cost of a single cyberhack

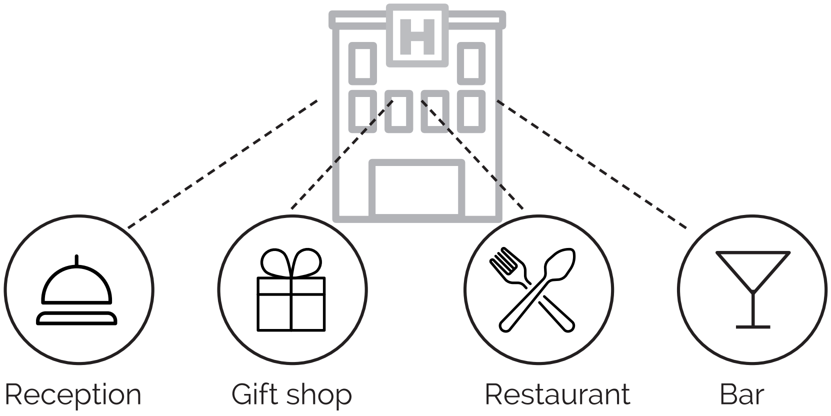
86%

of breaches **in the hospitality industry** occured at **small businesses**

What Makes the Hospitality Industry So Vulnerable to Cyber Threats?

There are several issues at play that make the hospitality sector a prime target for cyber criminals:

- Hotels and restaurants hold valuable client personal data, including customer names, mailing addresses, phone numbers, email addresses, and credit card information. Hotels may also store in their computer systems their clients' passport numbers, driver's license numbers, rewards account information, dates of birth, arrival and departure information, reservation dates, and communication preferences. All this information can be sold on the dark web. According to the New York Times, about $1 billion is lost due to crimes related to loyalty/rewards programs. Cyber criminals will use stolen credentials to impersonate customers, while others will sell the points online.
- Many hotels and resorts employ interconnected technology at their different locations linking gift shops, restaurants, and bars on their on-line platforms, making them even more of a lure for hackers. If a cyber criminal can get into just one location's gift shop or front-desk system, they can access a great deal more. If a hotel is connected to a restaurant, the data of both operations could be compromised.



- Third-party vendor relationships pose a significant level of risk for the hospitality industry. Hotels and restaurants rely on third-party vendors for many of their key functions including to make payments. As a result, many hotels and restaurants have suffered a data breach through their Point Of Sale (POS) systems. Hotels also use third-party reservation systems, property management, maintenance, human resources, payroll and other services. All of these functions involve having access to hotel systems, and thus become a potential entry point for hackers. In lieu of directly hitting a hotel, compromising the system of a key vendor to gain access to client data has become a preferred approach among hackers.

- Human error is also common in the hospitality industry, exacerbated by minimal cyber security awareness among employees. Not every hotel or restaurant employee is vigilant and cautious about the potential dangers of data breaches. Additionally not all employees are properly trained on spotting potential hacking and fraud, whether it is a counterfeit credit card or opening an email with a suspicious attachment. Furthermore, high employee turnover, particularly in the hospitality sector, can make it difficult to properly train staff.

Common Cyber Exposures Against Hotels, Restaurants

- **POS Hacks**: Once malware has found its way into a POS system, cyber thieves can siphon unencrypted clear-text credit card numbers and customer names. Experts say that POS data breaches are the “single biggest” cyber threat to the hospitality industry, as they offer the most direct route to credit cards and financial gain.

- **Data Breaches and Theft of Personally Identifiable Information:** With thousands of guests staying at hotels over time, there is a huge amount of customer data laying dormant in databases, website cookies, and devices – all ripe for cyber criminals to get their hands on.

- **Spearphishing Attacks:** One common tactic used by cyber criminals involves calling a hotel to complain that they are unable to make a reservation on its website. The phisher will ask to email his details to the employee with whom he is speaking. The hacker then follows up with an email containing a malicious file and waits until the employee confirms they have opened the file. With the malicious tools deployed, the hacker can enter the hotel network.

- **Wi-Fi Network Attacks:** Although security has improved in this area with better password management, attacks on public Wi-Fi networks at hotels still occur. Through a hotel’s Wi-Fi system, hackers can access guests’ laptops or mobile phones in order to use malware to infect guests’ devices, hijack their data, and steal passwords to their bank or other accounts and more. Hackers can also breach the hotel’s Wi-Fi system to steal databases of guests’ information if its system is not properly secured.

- **Ransomware:** This cyber threat has spiked in the last several years with hackers penetrating an operation’s system in order to install malware, take control of the organization’s network and hijack its data until payment is made.

$

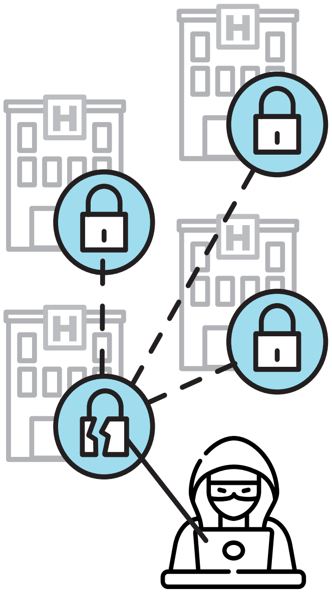
AVERAGE COST OF ATTACK.

Personally Identifiable Information	$3.92M
Spear phishing	$1.8M
Ransomware	$133K

Cyber Claim Examples

Following are several real-life cyber claims that have occurred in the hospitality industry:

- One of the five most significant breaches in history, the Marriott cyber attack identified in November 2018 compromised the data of hundreds of millions of guests who had stayed at Starwood Hotels & Resorts since 2014.
- In October 2017, Hyatt Hotels Group reported a massive payment data breach when credit card data was hacked from 41 Hyatt properties across 11 countries.
- A major hotel brand reported a breach in both 2008 and 2010, disclosing that cyber criminals penetrated the operation's central reservations database by hacking a single franchised hotel. The hackers used this connection to the hotel's central system to steal about 600,000 credit card records from other franchised hotels in the brand.
- A Mexican restaurant chain's data was compromised after cyber criminals accessed payment card details of customers through malware installed on payment processing systems at some of its locations. The compromised data included customers' names, credit card numbers, expiration dates, and verification codes.
- A restaurant management company was hit with a ransomware attack resulting in the establishment having to use backups to restore operations to its managed facilities, which took several days. While none of the restaurant's revenue operations were hindered, the attack required reconstruction of back office data, forensics and legal review.

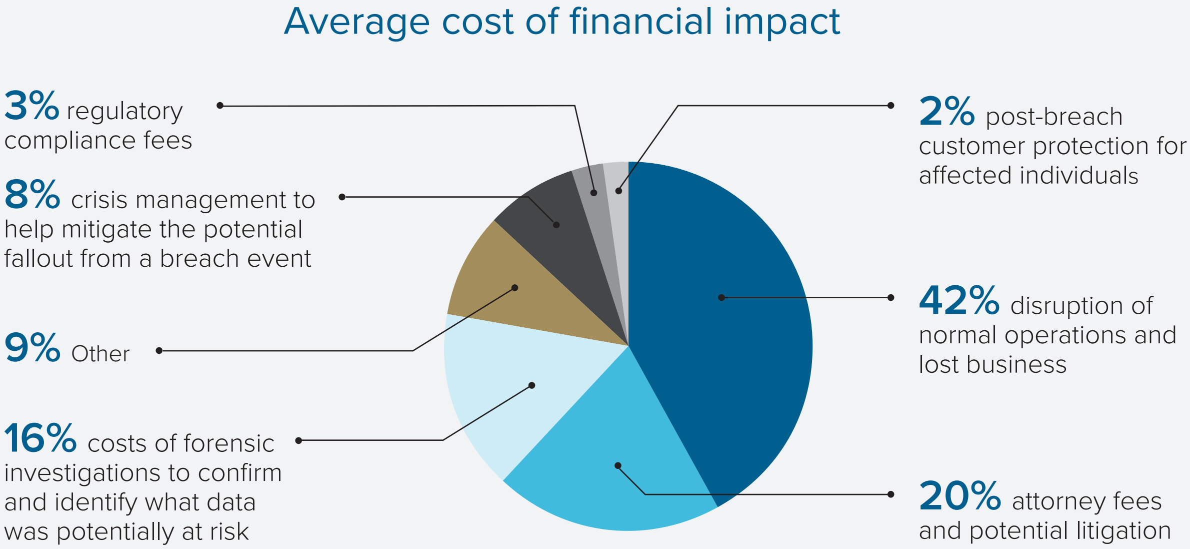


600,000

stolen credit card records

Impact of a Data Breach

The impact of a cyber attack can be far-reaching and devastating for a hotel and restaurant operation. You have the immediate financial impact from a breach, which may include



An establishment can also experience long-term effects from a security breach, including lost customer loyalty, which can have a lasting impact on profitability and share value; devaluation of the brand; loss of future business contracts and relationships; and liability exposure for the organization's executives and board members. Customers, shareholders, and government regulators want assurance from directors and officers that they are taking measures to mitigate and prevent breaches.

Putting Best Practices on the Table

Hotels and restaurants make cyber security a top priority in order to safeguard their own data and that of their customers. Following are several best practices to help mitigate and prevent today's growing cyber threats.

1. Have a process in place to patch and update systems from vulnerabilities as frequently as possible to remain adequately protected.
    - For example, implement a process to ensure that no unauthorized/malicious programs can be executed on the POS without detection.
2. Make daily backups and duplicates of data and files that can be retrieved in the event of system compromise or ransomware.
3. Install and regularly update anti-virus, network firewall, and information encryption tools to scan for and counteract viruses and harmful programs; guard against incoming network or denial-of-service attacks; and keep sensitive information safe.
4. Employ strong password management. Get rid of default passwords and make sure every staff member has his or her own login; ensure all hotel guests have unique passwords when accessing Wi-Fi.
5. Utilize multifactor authentication before authorizing any major, uncommon, irregular, or allegedly time-sensitive requests.
6. Provide regular, up-to-date training for staffers on the latest online threats and trends in cyber crime. At least 95% of reported data breaches could be traced to an intentional or unintentional act by a person within – or associated with – the affected organization.
    - Instruct staff about the dangers of clicking on unsolicited email links and attachments, and the need to stay alert for warning signs of fraudulent emails.
7. Conduct ongoing vulnerability testing and risk assessments on computer networks and applications to seek out and address possible points of failure before they arise. An organization may consider seeking a third-party provider to conduct vulnerability checks and provide recommendations for improvement.
8. Ensure all vendors meet a compliance standard, and regularly assess the risk of vendors and partners.
9. Have an incident response plan in place if a data breach does occur, which will help facilitate the communication and mitigation process.

Cyber Insurance & Risk Management

Along with strong cyber security measures, it’s critical for organizations in the hospitality industry to secure Cyber Liability insurance that provides the following:

- Third-party coverages to protect against losses to customer systems and data
- First-party coverages to cover losses as a result of a compromise to an organization’s system and own data
- Social engineering and e-crime insurance.

Along with the key protection these coverages offer – from paying for forensic and notification costs, legal and public relations expenses, fines and penalties, to covering loss of business income and cyber extortion expenses – it’s also critical to work with a carrier that provides risk management services. These services are instrumental in assisting an organization to mitigate potential losses and provide the expertise and support required if and when a loss occurs.

Distinguished Programs provides comprehensive, competitively priced Cyber insurance for the hospitality industry. Our program is written with cyber industry leader Beazley and provides all policyholders with the Beazley Breach Response Team’s 24/7 claims phone line and the Beazley Breach Response Information Package, which consists of numerous risk management tools including webinars and training tools.

The hospitality industry has emerged as a prime target for cyber criminals. New technologies that improve hotel and restaurant operations and elevate customer service also create additional potential opportunities for cyber criminals and the risks they pose. Understanding these risks, training employees on the risks, implementing strong cyber security, and securing insurance are all critical in protecting an organization’s business.

Sources: PwC, Upserve, Verizon, Hotel Management, IntSights