INTERNATIONAL JOURNAL OF GAMING HOSPITALITY TOURISM (IJGHT)
STOCKTON UNIVERSITY

Marino, M. (2025). Cybersecurity Threats and Their Impact on the Hospitality Industry. *International Journal of Gaming Hospitality and Tourism.* 5(1).
https://stockton.edu/light/documents/ijght_vol.5no.1/cybersecurity_threats_and_their_impact_hospitality_industry_9.8.25.pdf

Cybersecurity Threats and Their Impact on the Hospitality Industry

Marianna Marino
Student
Stockton University
marino17@go.stockton.edu

ABSTRACT
The multitrillion-dollar hospitality industry faces many cybersecurity threats due to its collection of sensitive data and technological growth. Cyberattacks, such as ransomware, data breaches, phishing, and DDoS attacks, capitalize on vulnerabilities in infrastructure, poor employee training, and lack of vetting supply chains. This leads to financial losses, reputational damage, and sometimes legal consequences. High-profile breaches, like those of Marriott and Starwood, express the urgent need for strong cybersecurity measures. The purpose of this industry commentary article is to examine and evaluate the impact cyberthreats have on the industry as well as solutions and strategies for risk reduction and preventive measures. This paper evaluates the root causes of these cyberthreats as well as insufficient frameworks and lack of response plans that impact stakeholders, including consumers, businesses, and employees. By prioritizing cybersecurity in the hospitality industry, companies can mitigate risks, protect stakeholders, and ultimately maintain their customers' trust.

Keywords
Cybersecurity, hospitality industry, cyberattack, hotel, market, customer, reputation, data breaches, risk

INTRODUCTION

The hospitality market is a trillion-dollar industry that globally reached over $4.7 trillion in 2023. This was forecasted to grow to at least $5.5 trillion in 2024, showing the industry as a prime target for cyberattacks due to its fast-growing market and extensive collection of guest data (Statista, 2024). A cyberattack is an attempt by hackers to damage or destroy a computer network or system (Oxford Languages, n.d). These breaches can include credit card information, email addresses, names, phone numbers, physical addresses, and demographics such as age, gender, and preferences. These cybercrimes are rapid and becoming more normalized with cybersecurity ventures predicting a 15% annual increase in cyberattacks until 2025 with the costs reaching $10.5 million (Cloke, 2024). Already, one-third (31%) of the hospitality industry has experienced a data breach at some point in their company's history. These breaches average about $3.4 million each and create irreparable damage to the hotel's reputation (Cloke, 2024). Eighty-nine percent of these companies experience repeat breaches, showing how pivotal cybersecurity is for protecting customer and consumer data, as well as protecting reputations that can be so easily damaged (Coursera, 2024).

Cybersecurity is known as the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this (Oxford Languages, n.d). Most cyberattacks that cybersecurity protects the industry from are DDoS, phishing, network breaches, ransomware, etc. These attacks highlight the importance of implementing and maintaining a strong cybersecurity program throughout properties so there are no more cybersecurity failures. These failures can be as simple as failing to ensure employees have strong passwords, not patching outdated systems or software, and lacking detection of unauthorized activity and firewall controls. It can contribute to a bigger issue, hotels falsely guaranteeing the use of appropriate security and safeguards. Customers will then feel misled and deceived, leading to lawsuits and settlements (NGE, 2024).

The purpose of this industry commentary analysis is to evaluate how cyberattacks impact the hospitality industry, examine the industry's stance as technology becomes more powerful, and analyze how cybersecurity can be improved. This article will then look at ways to reduce risks as well as long-term solutions for the hospitality market.

INDUSTRY CONTEXT

The hospitality industry is home to businesses in multiple categories, including entertainment, recreation, food and beverage, and lodging. This market collects various types of data that exemplifies vulnerabilities the industry has as a whole. One of the first threats that are expected is DDoS, or distributed denial of service, which is when attackers overrun a system with connection requests to the point that the volume exceeds the system's capabilities. Following is phishing, which is a cyberattack that occurs through emails that pretend to come from a trustworthy source. The email tricks the recipient into giving personal information and other details. Network breaches, which are the most common, often happen when guests are provided wireless internet service. The wireless internet service opens the possibility of malware and "spoofing" access points to grant criminals information. The last one, ransomware, allows criminals to deploy malware to infect systems and files and lock staff and businesses out. The criminals then contact the company demanding a ransom so they do not expose or destroy confidential information (Coursera, 2024).

Each one of these cyberattacks, plus ones not listed, can cause a ripple effect that leads to a loss of trust and significant damage in terms of the brand reputation and revenue losses.

An article released in October 2024 by the Federal Trade Commission discusses how the FTC took action against Marriott and Starwood due to multiple data breaches. The three large breaches happened from 2014 to 2020 and impacted 344 million customers throughout the world. The FTC then decided that Marriott International Inc. and its subsidiary Starwood Hotels & Resort Worldwide LLC would have to implement a new data security system. The settlement stated that Marriott and Starwood would provide all of their U.S. customers with an option to delete personal information stored in their database with regard to emails and loyalty rewards numbers. In addition, the settlement required Marriott to review and restore stolen loyalty points. Under a separate settlement, Marriott is required to pay a $52 million penalty to 49 states

and the District of Columbia to resolve data security allegations. The director of the FTC's Bureau of Consumer Protection, Samuel Levine, said, "Marriott's poor security practices led to multiple breaches affecting hundreds of millions of customers" (FTC, 2024).

Marriott is in charge of 7,000 properties throughout the U.S. and 130 countries. Marriott acquired Starwood in 2016 and took on responsibility for both brands. The FTC said Marriott and Starwood deceived their customers by claiming to have reasonable data security but failed to implement appropriate password controls, firewall controls, access controls and multi-factor authentication. The first breach happened in June 2014 and stole credit card information from more than 40,000 Starwood customers. This breach stayed undetected for 14 months until customers were notified in November 2015, when Marriott announced the merger of the two companies. The second breach started in July 2014 and went undetected until September 2018, in which criminals gained access to 339 million Starwood guest account records and 5.25 million passport numbers. The third, and last, was from September 2018 to February 2020, in which 5.2 million Marriott guests' records worldwide were compromised, including names, mailing addresses, email addresses, phone numbers, dates of birth, and loyalty account information (FTC, 2024).

The settlements included that Marriott and Starwood were prohibited from misrepresenting how they collect, maintain, use, and delete personal information. They must implement a policy to retain information only for as long as necessary to fulfill why it was collected as well as give reason for the data being collected. They must also establish and implement a security program that contains robust safeguards and undergoes independent third-party assessments every two years. Lastly, Marriott and Starwood must certify compliance with the FTC annually for 20 years (FTC, 2024). Marriott and Starwood are a prime example of the issues individual hotels in this market face with cyberattacks. It brings up the analysis of the real costs that any hospitality sector can go through when there is a security breach. This can encompass drops in stock price, terminations from negligence, lost revenue, lawsuits, fines, government investigations, and loss of reputation (Chin, 2024).

The root causes of cyberattacks in the hospitality industry originally stem from a large collection of guest data that is sensitive, personal, and sometimes financial. Insufficient cybersecurity exacerbates the vulnerabilities of a company, while supply chain risks from third and fourth parties add another layer. Additionally, the lack of employee training in cybersecurity allows for the recurrence of breaches without response plans to improve it.

These causes have consequences for various stakeholders, the main one being consumers. When a consumer's data is hacked, they face identity theft, financial losses, and a breach of trust. Businesses face damage to their reputation, revenue loss, and possibly closure. Lastly, employees face an unstable work environment, a decline in morale, and increased stress. These issues require a thorough analysis to strengthen the entire industry's cybersecurity and protect all stakeholders involved.

DISCUSSION

Through a review and examination of cyberattack data as well as the industry's cybersecurity methods, it is very possible to have the industry and its consumers be protected. For companies in the hospitality market to improve their security stance, they should focus on two things, preventing cyberattacks and mitigating data breaches. It is more ethical to invest in preventive measures than to respond once an attack has occurred, showing prioritization of not only consumers but the organization itself.

Implementing the best security practices as well as continuous monitoring, assessment, and adaptation will limit the cost and damage of successful attacks. Cybercrime is constantly evolving, meaning the hospitality industry has to evolve with it, especially to be more cost effective (Chin, 2024).

Steps the industry can take to prevent cyberattacks are risk assessments, cybersecurity frameworks, staff security training, updating software, threat intelligence, strong passwords, data limitation, and supply chain risk assessment, among others. Risk assessment is mentioned first because depending on the company, each individual enterprise will have different cybersecurity due to its size, location, etc. Gathering information about the cyber threat shows the company's stance and will help make accurate decisions about reducing cyber risks. These need to be performed regularly for each company to stay protected. Using a cybersecurity framework can help a business develop the perfect system and protect its customers, employees, and business partners (Chin, 2024).

A major prevention that is unfortunately overlooked is cybersecurity training for employees. Data breaches are known for involving some type of human error, which is a vulnerability for any company. It can be as easy as accidentally clicking a link or sharing access credentials with the wrong person. The key lesson while training members of one's staff is to have them understand why cybersecurity is critical in addition to being trained properly to use a point-of-sale system securely.

A POS system is one of the biggest vulnerabilities the industry has, making specific training in these aspects beneficial. The training should include logging out of devices, using and updating strong passwords, keeping access credentials private, how to recognize phishing emails, and reporting odd activity. Additionally, software must be updated regularly to ensure vulnerabilities are mended as quick as possible (Chin, 2024).

Furthermore, threat intelligence will keep hotels up to date on the latest hacker interests and cyber trends. The hospitality industry is specifically targeted by professional cyberattack groups, so knowing how to counter these activities is essential. One of the best ways for a company to improve its security is by making sure staff have strong passwords, which includes alphanumeric characters, symbols, and numbers. Such passwords are typically very difficult to crack and leave the attackers with nothing. Hackers cannot gain information if there is no data to be compromised, so limiting the amount of data being retained will significantly lower the impact of a data breach. Likewise, having a company use a supply chain risk assessment is essential in

performing top security measures. A business' attack surface extends to its suppliers and those who supply its suppliers, etc. It can be difficult to assess and monitor these third- and fourth-party suppliers, but it is essential due to each link in the supply chain having significant risk. By vetting third-party vendors and limiting the use of third-party apps, the hotel market can reduce its risk of data breaches remarkably (Chin, 2024).

The goal of the hospitality market is to avoid data breaches, even though they are very common. Every organization should have a plan for how it will respond to data breaches to save itself from substantial financial losses, the loss of its reputation, or even closure. An incident response team with a direct leader who knows the stakeholders' roles, responsibilities, and contact details would be beneficial. The team should include managers and executives from different parts of the company, such as the chief information security officer and the head of IT security. This team would then come up with an incident response plan that documents the steps the business would take after a cyberattack. The plan would include the response team's individual responsibilities and a set of guidelines with details that anyone in the company could adhere to. It's proven that companies with response plans have lower costs after a data breach due to them reacting more quickly and effectively. It is easier to identify the problem, contain the breach, inform partners and staff, make an announcement to customers, and work with authorities to end the cyber threat (Chin, 2024).

It is important for companies to also have backup data, event logs, anti-malware, and firewalls. Backing up critical data is essential if there is a need to restore business functionality in case of ransomware attacks. It is also beneficial to keep logs of who uses a network at any time so if it is needed to be analyzed by professionals they can find valuable information. Anti-malware is a layer of defense against cyberattacks as well as firewalls, which filter everything that tries to enter or leave a network. Stats show that 83% of breaches come from external factors, 95% are financially motivated, and 26% of incidents involve credential access obtained through brute force (DBIR, 2023). No company in the hotel market is safe, showing the need to enhance their cybersecurity to ensure their safety, as well as that of their employees and customers.

CONCLUSION

The hospitality industry is a significant contributor to our economy, therefore making it a vulnerable market for cyberattacks. As emphasized throughout the analysis, breaches can cause devastating financial losses, damage to reputations, and operable disruption. This highlights the critical gravity of robust cybersecurity measures, from preventive strategies, risk assessments, and staff training to cyberattack response plans. The industry has to be proactive in addressing the challenges it faces as technology changes each and every day.

The industry commentary analysis examined real-life, high-profile cases, such as Marriott and Starwood, to illustrate the real costs of inadequate cybersecurity and the necessity for companies to prioritize the protection of their organization. Adopting a new culture of cybersecurity awareness and advanced security systems, the industry can mitigate risks and maintain operational integrity. As cyberthreats continue to grow, it is vital to the hotel market to evolve with it. This article provided practical solutions to help the hospitality industry be more secure and equipped through trying times. Some solutions given were risk assessments, cybersecurity

frameworks, data limitation, supply chain risk assessments, staff security training, strong passwords, threat intelligence, and updating software. Employee training was one of the dominant security steps due to its adaptable implementations, such as online workshops or in-person classes. This training coincides with the other solutions and gives a more in-depth approach to all of them. An example is enacting regulations to back up an organization's systems data every 2-3 weeks minimum. Investing in these preventions will provide the industry new ways to not only protect its assets but maintain the trust of its customers around the world.

REFERENCES

2023 data breach investigations report (DBIR) | inquest. (n.d.). https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf

Cloke, H. (2024, September 12). *The 10 biggest challenges facing the hospitality industry in 2024*. Growth Engineering. https://www.growthengineering.co.uk/hospitality-challenges/

Competition, B. of, & Staff in the Office of Technology and the Division of Privacy and Identity Protection. (2024, October 9). *FTC takes action against Marriott and Starwood over multiple data breaches*. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/10/ftc-takes-action-against-marriott-starwood-over-multiple-data-breaches

Cybersecurity in the hospitality industry: Challenges and solutions: Upguard. RSS. (n.d.). https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry#:~:text=Supply%20Chain%20Risk%20Assessment,hotel%20management%20or%20online%20bookings.

Cybersecurity in the Hospitality Industry: Your 2024 Guide. Coursera. (n.d.). https://www.coursera.org/articles/cyber-security-in-hospitality-industry

Cybersecurity risks and regulatory challenges impact hospitality industry. Cybersecurity Risks and Regulatory Challenges Impact Hospitality Industry - Neal, Gerber & Eisenberg Website. (1970, January 1). https://www.nge.com/Insights/216304/Cybersecurity-Risks-and-Regulatory-Challenges-Impact-Hospitality-Industry#:~:text=Almost%20one%2Dthird%20of%20hospitality,report%20by%20cybersecurity%20provider%20Trustwave.

Oxford languages and google - english. Oxford Languages. (n.d.). https://languages.oup.com/google-dictionary-en/ Published by Statista Research Department, & 22, A. (2024, April 22). *Global market size of the hospitality industry 2023*. Statista. https://www.statista.com/statistics/1247012/global-market-size-of-the-hospitality-industry/#:~:text=In%202023%2C%20the%20global%20hospitality,trillion%20U.S.%20dollars%20in%202024