SAMPLE CASE STUDY STUDENT REPORT – UH Maui College

Discussed with students in the Hospitality and Tourism Program

Case Study on the Challenges for Perimeter Security in Hotels and Hospitality Locations

Problem Statement - *Hotels do a good job of ensuring their servers are secure from direct cyber-attacks however cybercriminals are focusing their attention on the hotel's untrained employees by utilizing phishing methods.*

RQ1 – What are the challenges faced by the Hospitality Industry in balancing the need for taking care of tourists and visitors, as opposed to provide perimeter and other security mechanisms to block unwanted physical and online intrusions?

RQ2 – How can effective physical and perimeter security be implemented without adversely impacting the visitor experience or need for open and welcoming spaces and environments?

Cyber and Perimeter Security in the Hospitality Industry

STUDENT NAME

UH Maui College

Table of Contents

Introduction

While civilians have no legal duty to protect one another from bodily or personal harm, hotels have a duty to ensure the physical safety and wellbeing of their guests. Hotels must practice a high level of care to protect the external and internal customers from third party threats. This seems like an endless list of liabilities and a high amount of compensation that may possibly be given out in the form of legal proceedings or immediate customer good will gestures but it does not end there. Hotels do not just try to keep their employees and current in-house guests safe from the elements and physical harm but also must consider the public risk. The public risk is that hotels are usually open to the public and any person can walk on to the property to have a look, enjoy the space, or to look for opportunities.

Any in fracture in the assumed safety can trigger consequences such as litigation and damage to brand recognition, this all equates to a loss of revenues for the property and other intangible costs. In summary this means that the hotel is expected to take more stringent safety measures as the likelihood of events happening arise. Every property will have their own level of risk and the methods they implement to keep their guests safe. Once anyone from the public steps foot on to the premises, the hotel then becomes responsible for the harm that they cause other guests.

The hospitality industry has experienced many cyber-attacks in recent years. Cyber-attacks are steadily growing and are garnering the attention of corporations as they are under constant threat. One of the most profitable activities for cybersecurity criminals lies in stealing credit card information as well as the information of the individual cardholders. Hotels, especially large properties that contains hundreds of rooms, can my mathematical calculation host tens of thousands and easily hundreds of thousands of customers in a matter of years and all this information is stored in the hotel's databases ("Cybersecurity Tactics," 2017). These databases then are likened to troves of honey pots for cyber criminals who want access to this information which can be exploited and sold afterwards. The databases hold information such as personal and mailing addresses, phone numbers, loyalty reward account information, travel information and private info such as email addresses. The information held in databases can be used to draw out a lot of assumptions about these guests staying at the hotel.

There is also the threat of emerging technologies which promise the rewards of efficiencies and change for traditional methods but also come with hidden dangers such as weak points that are exploited by hackers and other drawbacks such as points of entry in to the systems which may not be discovered until it is too late. These technologies may be physical or intangible, perhaps even sharing characteristics of both, but they may hold hidden liabilities for early adopting hotels which may choose to implement them too soon. A physical example of tech may be the standard room safe which can be reset by many means to gain access to it. A newer technology is mobile or keyless entry which uses hardware on the hotel's doors to interact with the hotel guest's hardware such as their smart phones. Starwood Preferred guest announced their app back in 2015 and has implemented it in their hotels.

Marriot has set it a brand standard across the board to have keyless entry for guests. One short example that has been experienced while working at Westin is that the mobile apps do present a security risk at a low level because the mobile application reveals the room number to the end user. This becomes problematic when it is coupled with the fact that room assignments may change leading up to the day and time of guest's arriving and checking in to their rooms.

This presents issues should the room assignment ever be changed to another room number or if the guest harasses the housekeeping or maintenance staff if guests are in a rush to prematurely enter the room they were assigned. The application reveals the room information such as room number location and attributes of the room such as size and view and so there is a possibility of this information being misused. Let’s not get in to the possibility of the faith being put on the mobile device and its ability to always open the door if software of hardware issues should arise. There is the possibility of mobile devices being left around the property and being lost or stolen which creates a liability that goes beyond the usual lost and found scenario of simply returning lost property to the guest.

Staff must be trained in all adoptions of new technologies whether they be physical or intangible. Cyber security is one aspect to be educated and trained on but there are also issues of social engineering which lies in the simple act of misleading or manipulation to get internal staff to release confidential or personal information that can be used for fraudulent purposes. There are many ways in which this can happen which we may get in to later. Social engineering aside there are other cybersecurity vulnerabilities present in hotels which can be decreased by training employees and keeping them updated on changes in regulations and safety practices developed by authorities.

One example of these vulnerabilities is the POS system or point of sales system as mentioned earlier with credit card fraud. An employee at Marriot for example will have regular trainings to ensure that they are being PCI DDS compliant (payment card industry data security standard compliant). PCI compliance training gives employees the knowledge they need to ensure that they are protecting both the consumer and the business by maintaining a secure environment for payment systems.

Background

The topic being researched has to do with perimeter and cyber security in the hospitality industry. Perimeter security is defined by the natural or manmade barriers, walls, and other systems used to keep individuals in and/or intruders out of a determined boundary. Cyber security is defined as being protected against unauthorized use of electronic data that was not authorized by an owner of said data, and any methods used to access unauthorized data. The importance of researching these two general topics is that as technology increases and more information becomes digitized and storied digitally, the opportunities and rewards for criminals and malicious individuals to benefit from access to the data increase as well. Any institution that holds responsibility for the safety of people or artifacts within their property also must ensure that they are taking the measures needed to safeguard what is under their care.

These two topics are vital and yet pose a threat to the hospitality sector because as a business, hotels are expected to take on the safety of their guests. A guest can be defined as a paying guest who is occupying ae room or patronizing the services of a hotel such as a day spa or restaurant. Hotels must also ensure the safety of their employees as well. Hotels hold an abundance of personal and sensitive data that must be protected, and this is where the capabilities of the hotel to implement a secure environment both digital and physical come in to play. The reputation and brand image of the hospitality company is at risk when unfortunate events arise from the lack of planning, execution, and preparedness.

Reviewing the literature will be done in themes that have been brought up and identified patterns that arise from the readings. While perimeter security and cyber security are concerns for the retail, military, and other sectors, and there have been advances and challenges for every possible sector of business out there dealing with both topics, we will not be exploring the topics in a general matter and instead solely going in to detail on how both these topics impact the hospitality industry. We will also focus on recent challenges and developments that have occurred the hospitality industry.

Problem Statement

Hotels do a good job of ensuring their servers are secure from direct cyber-attacks however cybercriminals are focusing their attention on the hotel's untrained employees by utilizing phishing methods. Last year Hyatt reported that 41 of its hotels had been infected by malware and had an unknown amount of guests' credit card information stolen (Verizon, 2018)

Literature Review

Creating a culture of security

There is a lot of focus on protecting hospitality properties, their databases, and systems from breaches. Starwood Hotels and Resorts Worldwide, Hilton, Hyatt, and the Trump Hotel Collection properties have been subject to the spotlight in 2016 when they each experienced large-scale breaches of personally identifiable and financial data that they held on previous guests' stays ("Cybersecurity Tactics," 2017). Point of sales systems or POS are constantly used in front of the line operations and interactions between guests and employees. There have been increasing attempts to take advantage of the weak points in these systems in place to acquire cardholders' names, addresses, phone numbers, email addresses, credit card numbers, and expiration dates ("Cybersecurity Tactics," 2017). These POS systems are not always checked and maintained for vulnerabilities as often as they should be.

In the event of franchisees such as hotel owners who wish to franchise and license a name such as Westin or Sheraton for their property usually have access to regional and global databases which presents the liability of having one isolated breach affecting another franchising property across the country or internationally if they are also using the same system in their daily business activities. Oracle, a point of sales systems provider, has had one such event occurs where a model unit was breached and had affected 330,000 merchants ("Cybersecurity Tactics," 2017). It is worth noting that the information does not always come from point of sales systems but also come from records that the company keeps about their internal operations, their employees' personal data and sensitive information such as social security numbers, and birth dates,

Repercussions of breaches

Damages can be both tangible and intangible Tangible damages can be measured, calculated and reported accurately due to their nature of being tangible and having a physical aspect to measure. These can include compensation, fines, and legal fees. However intangible damage is often left to estimation and does not account for the potentially future loss in missed business, lost opportunities, and loss of reputation. It is one thing for a corporation to have to deal with these events and another for a one-off property to survive damages like this. As stated, earlier guests are expecting their physical and digital privacy and wellbeing when staying at a property and guests may sue, media coverage may follow, and the damage could be catastrophic to specific properties. The rise of social media can also spread word of the event and leave a lasting indention in the brand name.

One real life event that happened in 2017 is the mass shooting that took place on the thirty second floor at the Mandalay Bay hotel carried out by a lone gunman in Las Vegas, Nevada. The event lasted 11 minutes and killed 58 people and left 700 others injured (Gulliver, 2018). Since the attack, a whole year has passed, and people are still trying to recover from the event. Security professionals were left wondering how this would affect future events and the detail of security that would be needed moving forward. Since the attack the concert goers who were there the night of the attack have tried to sue MGM and the promoter of the concert Live Nation (Natour, 2018), It is understandable as to why they would try to sue as guests have an assumption to be kept safe while they attend the concert.

Social Engineering

In recent years it has been shown that protecting oneself with firewalls, antivirus, and anti-malware software packages are not enough to combat these attacks. Phishing still proves to be a popular alternative and a work around to many of the very well-fortified databases that properties have been actively ramping up to prepare themselves against the lessons learned by competitors and partners alike. Phishing in the hospitality industry can happen when a guest is targeting to give up sensitive information such as but not limited to credit cards and by also targeting internal employees to hand over credentials or give access to an unauthorized individual (Koegler, 2017). Phishing can happen in the form of an email where an employee could get an email asking them to "click on this" which then gives the attacker access to the system or sensitive data. Phishing can also happen to hotel guests before or after their stay, where the email claims to be the hotel chain asking for them to send payment information or other sensitive information. It should be noted that these digital documents are crafted very well and look legitimate and even come from email addresses that seem trustworthy and at times even similar to an email address within their own organization (Lord, 2018).Attackers can be very well prepared and thorough in their preparations as they may do investigative research on names of individuals with clout so as to be able to name drop a particular higher up in the company in order to have the employee comply with handing over sensitive information (Barker, 2016).

Limiting access based on an information management system outlining user rights is a great way to limit the information accessed by internal employees and contractors. This helps to control what type of sensitive data is accessible to individuals based on their hierarchy in a company and their job description which allows the hotel to retain the integrity and security of private information. Many corporations are huge and span around the globe with hundreds of thousands of employees and so they are required to ensure that dormant or past users no longer have access to sensitive information. The monitoring of employee data usage should also be recorded and tracked to analyze for abuse. While it may be very unlikely that an employee would tamper with a company's data it is possible for an internal employee to steal the data for profit or destroy it for person reasons such as revenge.

Educating the staff at a hotel in every department is also necessary to ensure that they do not fall victim to social engineering tactics either in person or through digital communications. It is a mistake to assume that only the front of the line employees who work face to face with hotel guests would be the only ones who need the training. Every department from food and beverage, IT, marketing, housekeeping, and even human resources must be well trained and made aware of the methods that are used to gain bits of sensitive information. Over time, these small pieces of information may be used to mislead other employees in to giving the malicious individual more of the sensitive information they are after. There have been cases of employees working at human resource departments losing their jobs because they had sent sensitive information through email that belonged to employees ("Demystifying Cybersecurity," 2018). At one point, hotels that are serious about protecting themselves do have to come to the realization that they will eventually have a breach or loss of data and that is because there are too many locations that are potentially weak such as systems that are in constant use and usually by employees with limited training or who may be careless. The issue of having external vendors for software and hardware also poses a threat as well (Kumar, 2018).

Perimeter security

One of the challenges of perimeter security at a hotel property is balance. As there is a difference between keeping intruders out and captives within a perimeter at a military compound that employing stringent control and a hotel property that must remain sensitive to the hospitality needs of the business. Barriers come in natural and manmade forms and they are both critical in ensuring the security of a perimeter. As defined above, perimeter security is defined by the natural or manmade barriers, walls, and other systems used to keep individuals in and/or intruders out of a determined boundary.

Perimeter security is essential to protecting a property and hotels need to ensure that they deliver a system that delivers the positive welfare and safety of guests. It is very important to ensure that the executive team works together with the security management to design a system that monitors the movements of individuals on property, puts barriers in place to limit access points to sensitive areas on property, and that uses the latest technology to maximize the safety of everyone (Arlotta, 2017). The way that hotels protect themselves, their employees, and guests from dangers such as potential intruders is using monitoring. A hotel uses a system of cameras which are directed to a single room where a security officer can monitor the movements around the hotel property and keep a close eye out for suspicious activities and individuals of possible interest. Video footage is always recorded and stored if it can be used to resolve issues, find lost items, identify people, or keep employees honest. Hotels also employ the use of biometric data to keep sensitive areas private and allow authorization to specific individuals (both internal and external employees) with the use of biometric data and passwords. A hotel also utilizes the help of human talent such as security guards to patrol the grounds, to recognize the guests and their safety, and to monitor the activity that takes place on property.

At the Kaanapali Ocean Resort Villas located in the Lahaina side of Maui, they utilize several methods to keep watch and monitor who enters and exits the property. One such method is the use of biometric data such as fingerprints in conjunction with unique identifiers such as an employee number. Every employee that has special or privileged access to sensitive systems and areas of the property are asked to register their fingerprints to be given a security fob that is used during that employee’s shift. A key fob is a piece of small hardware that has authentication programmed into it to grant access to hardware systems, data, and restricted areas. It is a form of authenticating that when used along with a unique identifying code gives that person wielding the fob the credentials to access these systems or areas.

There is a methodology of determining a perimeter of security called “Concentric Circles of Protection” and this is used by hotel properties to evaluate the level of security needed or available by constructing layers or rings of protection (Arlotta, 2017). In this model there are big circles that encompass a bigger area with smaller circles within the larger circles. The smaller circles then have even smaller circles within them and these finally end up to a smaller area such as a single guest room or a storage facility. This allows a property to evaluate what areas need varying levels of protection and different methods of protecting them from unauthorized access (Segal, 2015). Electronic fobs like the ones discussed earlier may be used. Another method of securing a guest room is to have electronic locks that operate independently from access control management software. This ensures that in the event of power loss those locks will not be down from service and will continue to work and to minimize the liability factors. Locks at the Westin Kaanapali Ocean Resort Villas run on a battery which is unaffected by power outages.

The above subjects offer an in depth look at how cyber security and perimeter security play an important role in the hospitality industry. As a side note, it is important for hotel chains and corporations to assess the risks of opening and operating properties abroad in different countries due to the political and cultural differences between the corporation's home country and the host country of choice. A lot of risk assessment goes in to deciding whether a property will be able to compete efficiently and provide its in house guests with a safe experience. There is a lot of legal and cultural difference when going abroad and hotels would prefer a country that operates with the law of the land as laws are governed and upheld. A hotel chain would not want to operate in a country that practices law of man where warlords, regimes, and dictators can rule as they see fit. External forces such as these have been on the radar as terrorism is reaching the western world from internal citizens and external visitors. This will eventually impact hotels and they must be ready to meet a possible future incident.

Most of the articles that were used for this writing and collected were within the last 3 years and a few as recent as several months ago. It can be trusted that the articles are not outdated and are relevant to the needs of today's hotel properties. There was a type of data that was very difficult to obtain, and it was relating to articles explaining which specific hotels were getting breached, the specifics of what was breached or stolen, how it occurred, and what changes were implemented after the occurrence. Speaking to industry professionals also produced no possible leads for such articles and the only information they would provide were stories they heard from peers at other properties around the country. Articles relating to that were very difficult to find. It is understandable that this kind of information would not be available to the public as it may reveal weak areas for similar hotels and possibly be more damaging to that hotel's reputation and brand image.

Findings

The contacts that I chose were front line employees, supervisors, and managers from various departments at the Westin Kaanapali Ocean Resort Villas. It was important to gauge the level of awareness and confidence of employees regarding cyber security and social engineering techniques. This is because the hospitality industry is a hotbed of opportunity for cyber attackers. It is a lucrative source of information as they hold valuable information about their customers and the information provides a route to attack those individuals directly.

The last few years were bad for the hotel industry as far as cyber security and sensitive data security was concerned. As of a few days after the final survey answers were coming in, I received various texts with links to news sites regarding the newly announced Marriott security breaches that just hit the headlines in August 2018. It seemed that since taking the survey, a lot of the employees across departments were now more aware of the security issues facing hotels and were interested to share the news they have found with others. This means that since taking the survey there has been a positive change in employees' interest and awareness.

When speaking to an IT and Security employee about the news regarding the Marriott Starwood hotel data breach, there was much to be talked about. When there is a breach like this it is possible for the information to be taken by individuals dealing with organized crime who sell the information. Reservation information such as customer preferences and what locations they like to frequent and how often they frequent those locations could be out there. Access to a network for a couple of years can realistically have access to the entire infrastructure of a company's database and know what the organizations does using their data. It is possible that the intruder may have had access to a lot of the Starwood and the Marriott properties because there was a recent merger this year. There was a recent transition of data that has been taking place with the Marriott and Starwood systems as Marriot finalizes the complete transition of its Starwood assets.

There needs to be an emphasis on the responsibility of organizations who store and are charged with protecting other people's data. The data breach was due to an individual who had access to data for several years. It is unfortunate that the security and privacy of the guests was not their priority. There could have been risk management by transferring risk to an alternate party such as payment processing vendor who specializes in managing and storing credit card information. From what I heard internally, the data was stored in house at those properties. As we have learned this semester with risk framing, and security procedures, this move to have data stored in house is a very elementary mistake to commit.

Analysis

I have compiled all the data and run some basic statistics on them. I have boxes below containing the average rating score and standard deviation for the 18 responses for each of the six scaled questions. All 18 respondents answered the initial six questions. The sum of the responses was just to see which questions the employees felt the least and most confident in. The standard deviation was used to create a 95% confidence interval.

With this confidence interval I can say with 95% certainty that the employee population at the KOR would have answered each question within the ratings of the confidence interval. For example, for question #7, I would say with 95% certainty that the percentage of employees at KOR who would have thought differently/become more aware about cybersecurity and social engineering after taking my survey would fall between 22% and 74%.

1) How confident individual employee was in their hotel’s ability to keep the private information of hotel guests out of the hands of unauthorized users. (answers were on a scale of 1-5)

Number of responses	18
Sum of Responses	65
Average score	3.61
Standard Deviation in responses	1.42
95% confidence interval	(0.69, 2.15) *95% of employee ratings would fall between these values

2) The level of familiarity with phishing techniques and techniques criminals employ to get access to information that the individual employees had

Number of responses	18
Sum of Responses	65
Average score	3.61
Standard Deviation in responses	1.24
95% confidence interval	(0.61, 1.88) *95% of employee ratings would fall between these values

3) How prepared, individual employees thought that they and their fellow coworkers across departments, were to identify phishing techniques

Number of responses	18
Sum of Responses	56
Average score	3.11
Standard Deviation in responses	1.23
95% confidence interval	(0.60, 1.86) *95% of employee ratings would fall between these values

4) How prepared, individual employees thought that they and their fellow coworkers across departments, were to identify in person tactics employed to get access to sensitive information

Number of responses	18
Sum of Responses	63
Average score	3.50
Standard Deviation in responses	1.50
95% confidence interval	(0.73, 2.28) *95% of employee ratings would fall between these values

5) How individual employees would rate their executive team's efforts on mitigating the threat to guest's digital and physical safety from other guests and non-guests walking in and out of the premises

Number of responses	18
Sum of Responses	63
Average score	3.50
Standard Deviation in responses	1.34
95% confidence interval	(0.65, 2.02) *95% of employee ratings would fall between these values

6) How likely individual employees thought other employees or guests are at trying to gain access to private or personal information stored at the hotel property

Number of responses	18
Sum of Responses	47
Average score	2.61
Standard Deviation in responses	1.33
95% confidence interval	(0.65, 2.02) *95% of employee ratings would fall between these values

7) Employees who's thinking about the importance of cyber security in hotels has changed after taking the survey

Number of responses	16
# Employees who's thinking has changed	11
% Employees who's thinking has changed	69%
Standard Deviation in responses	.48
95% confidence interval	(0.22, 0.74)

The percentage per rating per question is listed below. The scale of 1 was least and 5 being the greatest. Questions are same as above.

Rating (1-5)	Question 1	Question 2	Question 3	Question 4	Question 5	Question 6
1	11.1%	5.6%	11.1%	11.8%	11.1%	16.7%
2	11.1%	11.1%	16.7%	23.5%	11.1%	44.4%
3	22.2%	33.3%	38.9%	5.9%	22.2%	16.7%
4	16.7%	16.7%	16.7%	17.6%	27.8%	5.6%
5	38.9%	33.3%	16.7%	41.2%	27.8%	16.7%

It is interesting to see that 44.4% of correspondents responded with a "3" or less on confidence in their hotel's capability of keeping private information out of the hands of unauthorized users, 41.2% are very confident ("5") that they and their coworkers are prepared to identify social engineering tactics, and 16.7% of employees are very confident ("5") that they and their coworkers are prepared to identify phishing techniques. There was quite a gap in the preparedness for social engineering tactics and digital tactics.

Recommendations.

There needs to be legislation to address the huge success of the hospitality industry and the recent accomplishments they have had such as the largest hotelier mergers in history. This success of mergers and high traffic has increased risk to customer data. There should be international law developed to address the risks and the penalties for breaches. Because of the lack of legislation, there is not enough pressure on how hotels should handle and store data. It does not end there but there should be a large budget set aside for the ongoing operations regarding data security.

While free Wi-Fi at hotels is a great amenity it is also a possible vulnerable point and a source of valuable information for malicious individuals. We must be careful when using public open Wi-Fi hotspots. Hotel Wi-Fi can be used as a route in to the consumers staying at hotels. The information or data that is sent from device to the access point is broadcasted in every direction for anyone to collect and analyze. That poses a huge problem, but how easily is it to collect data from one of these? Free Wi-Fi is completely open, and it is not encrypted. Using the right equipment, anyone can pick up the information being sent across the air. Monitor mode makes Wi-Fi chipset able to pick up and receive information from anywhere regardless of where the data is going to client devices.

To address this issue the front desk should take a minute to explain best safety practices when it comes to hopping on to the public Wi-fi at hotels as there could be hot spots named to deceive guests in to thinking that they are logging on to the hotel's "secure" Wi-Fi.

The security director shared various high-level advice which can be used by the hospitality industry to ensure that incidents are minimized: This information might not be the easiest to understand or know how to carry out, but these are steps in the right direction for professionals in the industry to follow.

1) Hotels really need to understand their level of exposure and how exposed you are across different domains and the supply chain.

2) Ensure that there is the capability and the resources available to be dedicated to the risk of exposure.

3) There needs to be a framework of how you approach and respond to the risk. This means looking at the access controls all the way to the work culture in various departments in the hotel from top to bottom.

4) Have independent tests of the hotel's defenses to get a real-life probing of these defenses to see how strong they are.

5) Ensure there is a crisis plan and instances planned in the event of these risks happening.

6) Ensure you understand the legal and regulatory environment that the hotel operates in since most chains are international these days.

7) The hotel industry needs to collaborate with booking agents and other partners to work together to deal with the threats that face the hotel industry.

In conclusion, there is a lot to celebrate for the hospitality industry when it comes to their success and their expansions, but this comes at the price of higher risk as they are targeted by malicious individuals who want to get access to their valuable data. Political and social reasons are also probably behind the attacks as well, as there have been instances where the information stolen does not show up on black market websites for sale. Regardless the private information of consumers should stay private and it is the responsibility of hotels to earn the trust of their consumers with their data. Trust is earned, not given. These hotels rely on consumers to stay at their properties, for what good are hotels with empty and unused rooms?

References

General cybersecurity

Cybersecurity Tactics for a Hotel Industry that's Under Siege. (2017, 16 June). *Hospitality Technology.* Retrieved from https://hospitalitytech.com/cybersecurity-tactics-hotel-industry-thats-under-siege

Tore, O. (2017). Why Cybersecurity in the Travel and Hospitality Sector is so Critical? *FTN News.* Retrieved from https://ftnnews.com/technology/33559-why-cybersecurity-in-the-travel-and-hospitality-sector-is-so-critical.html

Koegler, S. (2017). How Hotel Cybersecurity Keeps Guests and Data Secure. *Security Intelligence.* Retrieve from https://securityintelligence.com/how-hotel-cybersecurity-keeps-guests-and-data-secure/

Demystifying Cybersecurity for the Hotel Industry. (2018, 18 June). *Bluephish.* Retrieved from https://bluephish.org/2018/06/18/demystifying-cybersecurity-for-the-hotel-industry/

Kumar, N. (2018). Cybersecurity in Hospitality: An Unsolvable Problem? *Paladion High Speed Cyber Defense.* Retrieved from https://www.paladion.net/cybersecurity-in-hospitality-an-unsolvable-problem

Kefgen, K. (2017). Cybersecurity: A Hospitality Industry Reality. *Aethos Consulting Group.* Retrieved from http://www.aethoscg.com/aethos_insights/cybersecurity-a-hospitality-industry-reality/

Who Takes Responsibility for Cybersecurity in Hotel?. (2017, 24 March). *Phocus Wire*, *Tnooz.* Retrieved from https://www.tnooz.com/article/responsibility-cyber-security-hotel/

Cybersecurity for Hotels: 6 Threats Around the Corner from your Property. (n.d.) *Social Table.* Retrieved from https://www.socialtables.com/blog/hotels/cyber-security-hotels/

Effective Cybersecurity Tips for the Hospitality Industry. (2018, 12 June). *Prologic First, My Cloud Hospitality.* Retrieved from https://www.mycloudhospitality.com/blog/effective-cyber-security-tips-for-the-hospitality-industry

Social engineering

Barker, I. (2016). Sophisticated Social Engineering Attacks Target Hotel Chains. *BetaNews.* Retrieved from https://betanews.com/2016/11/29/social-engineering-hotels-chains/

Social Engineering: What Your Guests Don't Know Could Hurt You. (2017, 25 August). *Cvent.* Retrieved from https://blog.cvent.com/hospitality/hotels/socialengineering/

Lord, N. (2018). Social Engineering Attacks: Common Techniques and How to Prevent an Attack. *Digital Guardian, Data Insider.* Retrieved from https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack

Dotsenko, J. (2016). What to Do About Social Engineering and POS Attacks in the Hotel Industry. *Trust Wave.* Retrieved from https://www.trustwave.com/Resources/Trustwave-Blog/What-to-Do-About-Social-Engineering-and-POS-attacks-in-the-Hotel-Industry/

Perimeter security

Arlotta, C. (2017). Monitoring: The Key to Perimeter Security. *Hotel Business.* Retrieved from https://www.hotelbusiness.com/monitoring-the-key-to-perimeter-security/

Segal, M. (2015). The 4 Cornerstones of Improved Hotel Security. *AS Solutions Forward Thinking.* Retrieved from https://assolution.com/blog/the-4-cornerstones-of-improved-hotel-security/

McGoey, C. (2018). Hotel Security Amenity Moves to the Forefront of What Guests Really Want. *Crime Doctor.* Retrieved from https://crimedoctor.com/hotel-security-amenity/

Hiller, S. (2017). Three New Threats on the Hotel Security Radar for 2018. *Insights.* Retrieved from https://insights.ehotelier.com/insights/2017/06/08/sky-touch-hotel-security-radar/

Tech affecting security

Williams, B. (2017). Hotel Rooms Safes: They May Not Be as Safe as You Think. *Corporate Travel Safety.* Retrieved from https://www.corporatetravelsafety.com/safety-tips/hotel-room-safes-they-may-not-be-as-safe-as-you-thought-they-were/

Manley, B. (2015). Issues Loom for Keyless Entry in Hotels. *Hotel News Now.* Retrieved from http://www.hotelnewsnow.com/Articles/25693/Issues-loom-for-keyless-entry-in-hotels

Hughes, K. (2015). Keep Guest and Their Belongings Safe and Secure. *Lodging Media.* Retrieved from http://lodgingmagazine.com/keep-guests-and-their-belongings-safe-and-secure/

Hertzfelt, E. (2018). 4 Things to Consider When Making The Move to Mobile Key. *Hotel Management.* Retrieved from https://www.hotelmanagement.net/tech/four-things-to-consider-when-making-move-to-mobile-key

Barrett, M. (2015). Hotel Keyless Entry. *Global Traveler.* Retrieved from https://www.globaltravelerusa.com/hotel-keyless-entry/

Relating to actual attacks

Venues, Hotels Consider New Security Measures After Las Vegas Massacre. (2017, 9 October). *CGTN America.* Retrieved from https://america.cgtn.com/2017/10/09/las-vegas-massacre-security-hotels-venues

Natour, R. (2018) Are Hotels and Outdoor Concerts Any Safer Since the Las Vegas Attack? *PBS News Hour.* Retrieved from https://www.pbs.org/newshour/nation/are-hotels-and-outdoor-concerts-any-safer-since-the-las-vegas-attack

Gulliver, A.W. (2018). Two Hackers Have Found How to Break into Hotel-Room Locks. *The Economist.* Retrieved from https://www.economist.com/gulliver/2018/05/08/two-hackers-have-found-how-to-break-into-hotel-room-locks

Perez, C. (2018). How Hackers Can Break into your Hotel Room with Ease. *New York Post.* Retrieved from https://nypost.com/2018/04/25/how-hackers-can-break-into-your-hotel-room-with-ease