International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

Cyber Security Implementation in Hospitality Industry

Chai Ming En[1], Intan Farahana Binti Kamsin[2], Zety Marlia Zainal Abidin[3], Hemalata Vasudavan[4]
[1,2,3,4] Asia Pacific University of Technology and Innovation, Technology Park Malaysia, Bukit Jalil, Kuala Lumpur, Malaysia
[1]TP055741@mail.apu.edu.my, [2] intan.farahana@staffemail.apu.edu.my, [3]zety@staffemail.apu.edu.my,
[4]hemalata@staffmail.apu.edu.my

***Abstract* — The widespread use of IoT in the hospitality industry has led in increase in the number of cyber security challenges faced by the hospitality industry, as well as the sophistication of the cyber-attacks. A lot of hotel organization do not conduct security audits or do so infrequently, exposing customers and the organization to the risk of data breaches. This research is aimed to identify the cyber security challenges faced by the hospitality industry and propose an applicable cyber security solution to prevent cyber security attack for hospitality industry. To ensure the reliability of this research, interviews and surveys data collection methodologies have been conducted with IT experts in the hospitality industry, hospitality staff, and hotel guests. The interviews will be conducted as one-by-one structured interview with cyber security experts from the hospitality industry. A large number of hospitality staff and customers will be interviewed to determine how well they understand cyber security in the hospitality industry by using survey data collection method. At the end of this research the cyber security challenges faced by hospitality industry, the advance cyber security technologies and the solution of handling hospitality industry cyber-attack have been identified. An overview of Hospitality Industry Cyber Security System has been proposed.**

***Index Terms* — Cyber Security System, Cyber Security Threats Faced by Hospitality Industry, Cyber Security Technologies, Hospitality Industry, Hospitality Industry Cyber Security System.**

1. Introduction

With the advancement of the internet, the hotel industry is constantly introducing and updating the latest internet of things (IoT) technology to provide their customers with a more enjoyable experience. With all of these conveniences come challenges for the hospitality industry, most obviously the importance of make sure the cyber security of these hospitality industry-integrated technology. Since IoT technologies using certain hotel applications require the collection of a large amount of information about customers, hotel staff and even third parties such as suppliers, databases in the hotel industry often store a large amount of private information. In the case of a data breach and information loss, the hotel might be responsible for a huge amount of compensation, loss of reputation, and loss of customer loyalty. To avoid such losses, the hospitality industry takes network security very seriously. The organizations should examine their networks for a range of security threats, such as computer-aided theft, spying, cyberattack, phishing, and system breakdowns, among others. Therefore, this research will be focus on the cyber security threats facing by hospitality industry and the cyber security technologies to prevent the cyber-attack.

2. Literature Review

2.1 Research Domain

2.1.1 The cyber security threat facing by hospitality industry

Cybercrime has occurred since the rise of the internet, but the form of attacks and crimes has changed as technology has progressed. Technology theft occurs when an attacker connects to a computer with the intent of stealing technical information. Theft of proprietary information happens when an unauthorized individual or company exploits confidential trade knowledge for third party such as other organization. When an attacker connects to a computer with fraudulent purpose or impersonates a legitimate user of a computer system, fraud happens. Hospitality industry should be responsible for any data loss as they could prevent data breaches and security breaches by implementing effective preventative measures [1].

Consistent data breaches in the corporate sector serve as a reminder to companies of the need of incorporating cyber security technology and approaches into their operations in order to prevent such disasters. Using various types of phishing emails, viruses, etc., the cyber attackers can exploit the systems of hospitality industry. If a hotel's staff lacks sufficient understanding in this area, for example, browsing an insecure website or clicking on a link in an insecure email might have disastrous effects [1].

Based on Arslan Muni research, the attackers are able to hack and exploit hotel Wi-Fi. This kind of cyberattack is also known as a DarkHotel hack. The majority of hotels provide free Wi-Fi to its visitors, and customers may use the same network throughout the hotel, including in the lobby, conference center, dining room, and other areas. If the hotel's Wi-Fi is not secure, as is the situation in the majority of modern hotels, hackers may monitor the visitors' Wi-Fi traffic and exploit it to steal their private information. Due to the apathy and carelessness, the absence of system updates of many hotels, these outdated software programs could be used by hackers to get private information from hotels.

In the hospitality sector, however, one of the most popular techniques of data breach is "Fake Booking," in which an attacker constructs and designs a website with the identical appearance and functionality of the official hotel website and uses the same name to claim it is the hotel's official website [1]. To persuade users that a software download is secure, the attackers fake digital certificates [2]. As a result, a large number of potential guests visit the phishing website, and some may even make the hotel reservation via the phishing website, this leads the attacker can expose the visitor's sensitive data and financial information.

DDoS is another common type of cyber-attack exploited on hotels worldwide. The attack was a distributed denial of service. Furthermore, DDoS is the exploit of option for those who want to attack many hotel systems used by hospitality industry. Common objects such as fire sprinklers and surveillance cameras are susceptible to hacking. After that, whole computer and networks system may be brought to system crash. All the hostel organization must provide a method for mitigating compromised systems in the event that they are brought down by a DDoS assault [2].

Attacks on point-of-sale systems represent the greatest danger for the hospitality sector. Not only targeting the hotels themselves, but also third-party crimes, i.e., the attacker will attack the suppliers. And it suggests somewhere there is a vulnerability in the system which has been uncovered by human mistake. One example of this is MasterCard payment an unknown institution for $1.4-million, and Visa roughly $500,000 [2].

Based on the researched articles, the attackers assaulted the hotel with the aim of gaining access to the hotel's network and crashing the whole hotel system, making it unusable. Through these attacks, the attacker is able to induce a data breach and steal private data, and by threatening the hotel, they are able to demand a large ransom.

2.1.2 Evaluate on current cyber security technologies.

The cyber security technology protects the network's privacy, integrity, and accessibility. Network security technology refers to the technical measures and administrative procedures that enable the protection of organizational assets and individual privacy via a network [3]. Network security is required to safeguard data and prevent network assaults. There are several best practices and cyber security technologies for implementing robust cybersecurity that decreases vulnerability to cyberattacks and protects important information systems without compromising with the customer experience.

Identity and access management (IAM) is one of the most advanced cyber security technologies available today. It specifies the roles and authorizations of each user, as well as the rules under which those privileges are given or refused. Single sign-on is a method of IAM that allows a user to log in to a network once without providing their credentials again within the same session. Next is multifactor authentication, which requires the use of two or more access credentials. In additional, IAM also employs privileged user accounts to offer administrative access to certain users. User lifecycle management is an IAM technique that controls each user's identity and access credentials from registration through retirement. IAM technologies may also provide your cybersecurity professionals with enhanced visibility into suspicious behavior on end-user devices, even endpoints to which they do not have physical access [4].

Apart from that, the Security Information and Event Management (SIEM) is one of the advance technologies for cyber security. It combines and analyses data from security events to automatically identify and respond to suspicious user actions. SIEM systems of the current day use sophisticated detection methods, such as analyst user behavior and artificial intelligence. SIEM may automatically prioritize cybercrime response in accordance with the risk management goals of the organization. There are many enterprises are connecting their SIEM systems with security orchestration, automation, and response (SOAR) technologies that further automate, expedite, and handle many cybersecurity issues without human interaction [4].

A firewall is a network device (hardware or software) that filters certain types of network traffic, creating a barrier between trusted and untrusted networks. A firewall is a hardware or application that prevents unwanted Internet traffic, such as known viruses, from entering computers that are protected. Firewalls enable network administrators to filter incoming and outgoing network traffic. A firewall's rules examine one or more packet properties, such as the protocol type, the source or destination host address, and the source port. Based on the stated rule, the firewall should take action on the packet, such as forwarding it, discarding it, etc. By default, the firewall should discard all packets if they are not explicitly permitted by the ruleset [3].

According to multiple articles, by adopting cyber security solutions may effectively secure data, reduce the risk of cyberattacks, and prevent cyber-attacks from accessing or damage systems. This provides customers and organization a significant level of privacy, integrity, and security for their asset.

2.1.3 Implement the cyber security technologies to solve the problem facing by hospitality industry

Users of information technology are susceptible to several security concerns including cyberattacks. The most frequent threats include malware, insider hackers for network access, spoofing, unauthorized insider and outside access, and DOS attacks. Cyber security seeks to maximize the profits and returns of organization by reducing the damage that might be caused by

security attacks. Information security systems aim to prevent the discovery or damage of important assets. There are a lot of methods, and approaches for information security to provide protection.

Digital Identifiers (IDs) is one of the cyber security technique, IDs are the equivalents of identity card in the digital form. Usually, digital IDs consist of a username and a password. A user or system in asymmetric cryptography (a kind of information security system) has both a public key and a private key, which may function as identifiers. In cryptography techniques, public keys and identifiers are authenticated via digital certificates. A certificate connects the identification of a user or system to its public key by delivering a digital signature over the public key and the identification of the user or system. This enables for extremely accurate differentiation between those who have access and those who do not have access to the hospitality industry network [1].

Apart from that, Intrusion Detection System is also a modern cyber security technique that applying in hospitality industry. It is a system that monitors events happening inside a computer and network system to detect malicious or threats. An intrusion is an effort to circumvent the system's security services, such as confidentiality, reliability, and authenticity. Typically, malicious actors' breaches are designed to launch a denial-ofservice assault that renders an organization's computer systems inaccessible. Intrusions can be caused by a variety of methods. First, intruders accessing from the Internet or other external networks. Second, authorized users seeking to get extra privileges for which they are not authorized. Third, permitted users misappropriating and abusing the privileges they have been approved. This technique allows a hotel's system to avoid crashing down during facing an attack's denial of service attack [1].

Other than that, the firewalls have always been an important component of network security in the hospitality industry. Network firewalls is one of the firewall types. It protects a whole network by monitoring the network's perimeter. Network firewalls forward and filter traffic between machines on an internal network depending on the administrator-defined criteria. There are two types of network firewalls: hardware firewalls and software firewalls. Firewall systems from CISCO, Juniper, and others safeguard the perimeter of a network by monitoring incoming and outgoing traffic [1].

In addition, the web application firewall (WAF) is one of the cyber security measures that hotels may use to prevent data breach threats. A WAF is different from a conventional firewall, it may monitor the content of certain web apps, therefore helping in the avoidance of malicious threats from web application security vulnerabilities such as SQL injections, buffer overflow etc. WAF technologies are also helpful to identify and mitigating data theft because, should an attacker target a credit card database, WAF solutions are able to identify and block the database [1].

Based on the researched articles, that prove that there are several cyber security technologies applicable to the hotel business. These include technology, such as Digital Identifiers (IDs), that are used when facing a cyber-attack. There are also technologies that need to be implemented before a cyber-attack, such as web application firewalls (WAF). All these technologies will protect the hotel from the damage and theft of valuable assets and data. When these technologies are applied to a system, attackers will not be able to easily penetrate hospitality's network because we have a firewall. If they are able to bypass the firewall, attackers will not be able to compromise the system with an unknown identity because we have IDs technology. Even if they bypass the IDs technology, they will be detected by the Intrusion Detection System.

3. Similar System

3.1 Intruder

Intruder is an enterprise-grade, cloud-based network security software bundle. It has a powerful scanning engine, making it appropriate for larger enterprises that want great protection without increased complexity. The vulnerability scanner of an intruder is continually on the search for newly discovered vulnerabilities.

Instead of forcing users to continually update the program, the tool is always linked to a secure remote server. Intruder scans the perimeter of the organization for anything that might expose databases or other resources to the public internet. If a violation was occurred, the organization would be immediately notified.

Intruder has a noise reduction module to guarantee that you only get reports on vulnerabilities that have an actual effect on the current security posture of the organization. The Cloud Connector module of the application enables connectors for all the most major public cloud platforms such as Microsoft Azure, Google Cloud, and Amazon Web Services (AWS). Other advanced vulnerability tools include the capacity to scan for common web application flaws and SQL injection.

Over 10,000 distinct forms of cross-site scripting attacks and other vulnerabilities are scanned for by the intruder. The Network View module that is included with Intruder makes it easy to monitor exposed ports and services. Intruder is compatible with most of the hardware setup. The user may download security reports in a different format or view them using any common web browser.

Figure 1:Dashboard of Intruder

Figure 2: SQL injection assessment of Intruder

Figure 3: Syxsense Overview of Inventory

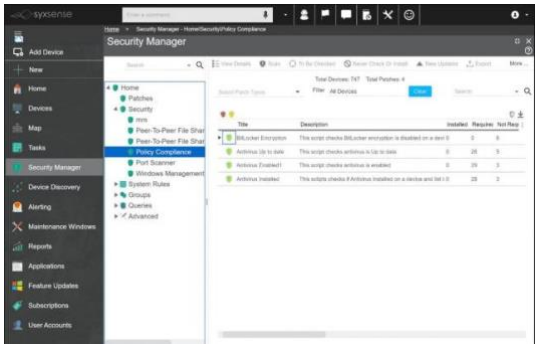

Figure 4: Syxsense Security Manager **3.3**

3.2 Syxsense

Syxsense is a cloud-based endpoint security software developed to assist IT administrators in maintaining threat avoidance by techniques of permission screening, third-party patching, communication blocking from infected devices, and constant team collaboration.

Compliance management, audit trail, file access control, application security, password management, vulnerability prevention, real-time monitoring, and maintenance scheduling are essential Syxsense features. In order to avoid cyber assaults, the security scanner provides managers with information regarding antivirus status, security implementation, and permission difficulties. Teams may also get real-time and precise information on RAM use, disc space, process monitoring, registry data, CPU usage, and more, which aids in identifying breaches of security requirements.

With security scans, Syxsense enables users to discover and remove threats by securing inadequate user account profiles and weak passwords. The technology enables IT workers to produce graphical reports based on the most susceptible devices, job summary, and security risk assessment.

Comparison Table

	Intruder	**Syxsense**
Suitable Organization	Small to large organization	Small to large organization
Category	Cloud-Based	Cyber Security Software
Pricing	$108/Per-Month	$960 per year for 10 devices.
Available User Amount	1-10 User	51-1000+ Users
Web Scanning	✓	✓
Vulnerability Assessment	✓	✓
Asset Tagging	✓	✗
Policy Management	✗	✓
Patch Management	✓	✓

Risk Management	✓	✓

Table 1: Comparison Table of Intruder and Syxsense

According to the Table 1, Intruder and Syxsense are suitable for small to large organization. The category of Intruder is Cloudbased Vulnerability Scanner which no need to keep updating the system, and for Syxsense is a cyber security software which mean might need to update after purchased. Both systems require a charge to use. The available user amount for Intruder are 1 to 10 people after purchased, Syxsense does not set too many restrictions, it allows 51 to 1000 + users to use it after purchased. The Intruder and Syxsense have a very wide range of features, such as Web Scanning, Vulnerability Assessment, Risk Management etc. However, the two systems also have features that are not present in each other. For example, Intruder has asset tagging and Syxsense does not. Syxsense has policy management and Syxsense does not.

According to the comparison, to propose a great hospitality cyber security system, Cloud-Based category has applied as the system category for the proposed system of this research. A Cloud-Based system can reduce the complexity of the system and make it easier for users to use the system. A great hospitality cyber-security system is required the basic vulnerabilities scanning, vulnerabilities assessment, patch management, notification when found vulnerabilities, etc. Not only that, but the features that are not present in each other will also developed to the proposed system, for example the asset tagging and policy management features. The asset tagging feature is providing the organization with a comprehensive review and track for their IT assets. The policy management enable the organization to reduce the risk. These features have developed in the proposed system of this research.

4. Problem Statement

Network security and cybercrime are most prevalent threats that the hospitality industry faces. While technological advancements and customer relationship management are being developed to enhance operational efficiency and customer experience in the hotel industry, it is clear that data breach incidents pose significant risks to the hospitality industry and its customers' privacy [5]. Unfortunately, the majority of hotels do not conduct security audits or conduct them infrequently, putting customers and the organization at risk of data breaches. As a result, there is insufficient planning and strategy regarding the impact of cyberattacks on the company's financial and operational performance, the hotel organization's readiness to avoid data breaches, and the ability to analyses and respond to adverse circumstances. The consequences of data breaches serve as a wake-up call for hospitality executives.

5. Research Aims

The aim of this research is to identify the cyber security threat of hospitality industry and propose the applicable cyber security solution to prevent cyber security attack for hotel.

6. Research Objectives

- To identify the cyber security challenges for hospitality industry.
- To evaluate the current cyber security techniques that applying in hospitality industry
- To propose a solution to handle cyber-attack of the hospitality industry network.

7. Research Questions

- How to identify the cyber security challenges that facing by hospitality industry?
- How does the current cyber security techniques applying in hospitality industry to secure the hospitality?
- What would be the solution to cyberattacks on the network of the hospitality industry?

8. Research Significance

This research will conduct to provide the hospitality industry with a better understanding of cyber security threats and solutions to these attacks and threats. The staff of hospitality industry especially for IT department able to scan the cyber security threat of their hotel management system. If there are any cyber security threat, the solution will be proposed for them. Not only that, the current cyber security technologies will be evaluated to propose a prevention such as firewall to protect the hotel management system. In short, by research the hotel industry's systems will be difficult for attackers to breach. Even if the system is compromised, the hotel's staff are well prepared for the attack since they already have a basic understanding of the cyber-attack they will face and the appropriate response.

9. Methodology

9.1 Target Respondents

The target respondent of this research are the hospitality IT experts which included the academicians, hospitality staff and customer. The reason for choosing a respondent with a background in cyber security is that they will give more professional answers to the threats and solutions faced in the hospitality industry based on their experience. The purpose of selecting the respondent without a background in cyber security is to analyses their knowledge of cyber security and the level of understanding of cyber security by the general population.

9.2 Sampling Method

There are 2 sampling methods will be applied in this research, judgment sampling is one of them. Due to this research desire to gain a deeper understanding of the solution and threats facing by hospitality industry, the respondents for this survey needed to have a cyber security background. Stratified sampling is the second sampling method, this sampling method is used for those respondents who have no cyber security background. In this research, the population have been divided into different subgroups with the similar characteristics. Every different role represents a different subgroup

9.3 Sample Size

This survey will be generated from the response of 100 respondents. These respondents are consisting of the hospitality cyber security experts which included the academicians, hospitality staff which included the managers, IT s department's staff and front desk clerks and the hospitality customer.

9.4 Data Collection Method

The data collection methods that will be used in this research are interview by qualitative research approach and survey by qualitative and quantitative research approach. The interviews will be conducted as structured interview and by one-to-one format by online meeting. This one-on-one interview is using to conduct interviews with cyber security experts, as the number of respondents with a background in cyber security is relatively small and there is sufficient time for one-on-one interviews. Not only that, qualitative research is highly suitable for exploratory purposes, so this interview allows the interviewer to delve deeper into the context.

The survey data collection method will be used on the respondents who without a cyber security background. Because there are a large number of respondents who have no cyber security background, with a survey the researcher can get the data from the large number of respondents in a limited time period. The survey will be distributed by online method such as email and google form. The types of questions in this survey will include open and closed question. The open question type will contain questions from the subjective question type and for closed question will include Likert-scale question with 5 points. For example, the Likert-scale question include "The company provides very adequate cyber security training" and rate it from 1-5 Strongly dissatisfied to Strongly satisfied.

9.5 Data Analyst Method

An ordinal statistic will be used on survey for closed question, The purpose of using this data analysis method is to summaries the non-mathematical data such as the satisfaction that gain from the survey and convert those in a statistic

9.6 Limitations

Poor response will be considered as a limitation of this research, this limitation will be more obvious in our survey collection method, since our survey is distributed to a large number of respondents via online, so there is no assurance that every respondent will respond the survey. To control the potential confounding factors, more effort was expended to distribute the survey to more correspondents. For example, our target sample size is getting 100 responses for survey, the surveys have been distributed to more than 150 respondents. **10. Overview of the Proposed System**

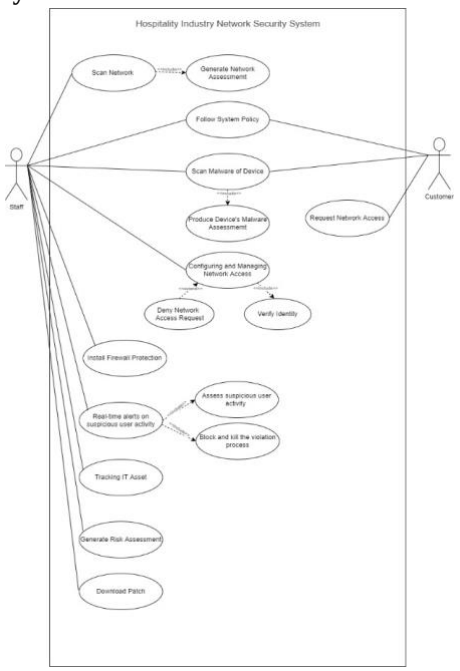

Figure 5: Hospitality Industry Network Security System

Figure 5 show the overview of the proposed system will be discussed in this section by a Use Case Diagram. In this research, a Hospitality Industry Network Security System will be proposed. The diagrams show two roles for using this system: staff and customer. Staff refers to the IT department employees who use the Network Security System, whereas customers are the hotel guests who request to use the network. The system will be developed as a Cloud-Based Network Security System with no restrictions on the number of users.

Several features have been proposed for the development of this network security system. The staff using this network security system are able to scan their network, after which a network assessment will be generated. In addition, a system policy management will be added to this system to introduce the process for when and how to use particular cyber security technologies during a critical event. Next, staff and customers will be able to scan their device, after which a malware assessment will be generated. Staff are able to configure and manage network access for the hotel's network. To gain access to the hotel's network, the applicant must verify their identity,

after which the staff can decide whether or not to allow access. Besides, this system will provide firewall protection and continuously update the firewall with the latest technology. In addition, the staff will receive real-time notifications of suspicious user activity. When the system detects suspicious user activity, it will send an alert, assess the situation, and block the violation process. The system also allows the staff to track the hotel's IT assets and generating a network risk assessment. Apart from that, the system will also provide patch management, allowing staff to download a specific patch to eliminate the vulnerability. Other than that, customers can request to use the hotel's network, for instance to access the hotel's Wi-Fi.

11. Conclusion

In conclusion, this study emphasizes the significance of cyber security to the hospitality industry. The study also identifies the cyber security challenges faced by the hospitality industry, the most advanced cyber security technologies currently available globally, and the most advanced cyber security technologies most suited for use in the hospitality industry. After investigated a huge amount of information, an overview of the hospitality industry's cyber security system was proposed. This system enables hospitality industry to have an better cyber precautions for their hotel, not only that it also enables the hotel's IT department to manage the hotel's network more effectively and stringently, and also enables hotel guests to determine whether their devices have been infected with malware

References

[1] Shabani, N., & Munir, A. (2020, July). A review of cyber security issues in hospitality industry. In Science and Information Conference (pp. 482-493). Springer, Cham.https://www.researchgate.net/publication/342683038_A_Review_of_Cyber_Security_Issues_in_Hospitality_Industry.

[2] Tables, S. (2022). Cybersecurity for Hotels: 6 Threats Just Around the Corner from Your Property. Social Tables. Retrieved 28 April 2022, from https://www.socialtables.com/blog/hospitality/cyber-security-hotels/

[3] Bahuguna, A. (2016). Advanced Cyber Security Techniques. Cemca.org. Retrieved 8 May 2022, from https://www.cemca.org/ckfinder/userfiles/files/PG_Diploma_in_Cyber_Security/Course%20VIII_Advanced_Cyber_Security_Techniques.pdf.

[4] IBM. (2021). What is Cybersecurity?. Ibm.com. Retrieved 8 May 2022, from https://www.ibm.com/topics/cybersecurity.

[5] Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: a need for cybersecurity risk assessment in the hospitality industry. Journal of Hospitality and Tourism Technology.. https://www.emerald.com/insight/content/doi/10.1108/JHTT-07-20170044/full/html?fullSc=1.

[6] Capterra. (2022). Comparing 2 Vulnerability Management Software Products | Intruder vs Syxsense. Capterra. Retrieved 5 May 2022, from https://www.capterra.com/vulnerability-managementsoftware/compare/161379-141605/Intruder-vs-Patch-Manager.

[7] Chigozie Nwokorie, E., & Igbojekwe, P. (2019). Security Challenges for the Hotel Industry: Implications for Selected Hotels in Owerri, Nigeria. Academica Turistica, 12(2), 193-205. https://doi.org/10.26493/2335-4194.12.193-205

[8] Ekransystem. (2022). Securing the Hotel Industry from Cyber Threats: Pandemic Lessons and 8 Best Practices to Improve Data Protection. Ekransystem. Retrieved 28 April 2022, from https://www.ekransystem.com/en/blog/cyber-security-in-hotels.

[9] Getapp. (2016). Syxsense Pricing, Features, Reviews and Alternatives. GetApp. Retrieved 5 May 2022, from https://www.getapp.com/itmanagement-software/a/patch-manager/.

[10] Intruder. (2019). Intruder - Research and Compare. technologyevaluation. Retrieved 5 May 2022, from https://www3.technologyevaluation.com/solutions/54206/intruder.

[11] Panai, E. (2018). A Cyber security framework for independent hotels. Proceedings 4th EATSA-FRANCE 2018, Challenges of tourism development, 145-152. https://www.researchgate.net/publication/325780143_A_Cyber_Security_Framework_for_Independent_Hotels

[12] Pande, M. N. R. (Ed.). (2016). Cyber Attacks and Counter Measures: User. Meta, 3, 1Attribution. https://uou.ac.in/sites/default/files/slm/MIT(CS)-103.pdf

[13] Shabani, N. (2017). A study of cyber security in hospitality industrythreats and countermeasures: case study in Reno, Nevada. arXiv preprint arXiv:1705.02749.