IRASA International Scientific Conference
SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION
SETI VI 2024
Book of Proceedings

DOI: `https://doi.org/10.62982/seti06.dula.56

THE IMPACT OF CYBER SECURITY ON PROTECTION IN THE HOTEL INDUSTRY

Dušan Laković[203]

Abstract

The paper aims to review the basic elements and guidelines for the application of cyber security concerning the increasing intensity of high-tech crime in the hotel industry. It is precisely the rapid growth of ICT in such an intensive activity as tourism, and especially in the hotel industry, that led to special types of protection such as cyber security. The application of ICT produced a series of abuses, which triggered a whole set of designed and coordinated measures to protect all participants from negative phenomena in this integral part of the hospitality industry. Cyberspace is an unsafe place, and knowledge of how ICT works, especially the world's most famous Internet network and the individual mechanisms of communication protocols attracts an increasing number of cybercriminals who exploit their vulnerabilities and carry out criminal activities. The hotel industry, as a part of the entire economic system and global business, is not isolated and follows the modernization trends of other industries, so in addition to the traditional ones, it enables new or complementary digital services where malicious users are constantly finding new ways to compromise security. In the research, the methods of analysis, synthesis, compilation, description and case law are used to adequately understand a complex phenomenon, such as cyber security, and propose courses of action. In this sense, it is necessary to design and manage such digital services, which enable mitigating the consequences of cyber-attacks in terms of breaching data confidentiality, availability and integrity, which is not easy.

Key words: *cyber security, hotel industry, cyber attacks, cyber protection*

Introduction

The rapid and comprehensive development of modern information and communication technology enables extremely fast communication services and more efficient business operations for individuals and numerous companies. Numerous new technological and technical solutions (Internet, mobile and satellite phones, Wi-Fi and other devices that can be connected to the Internet, better known as "things")

[203] Assitant Professor Duško Laković, PhD, Academician of IRASA, Ministry of the Interior of the Republic of Serbia, duskolakovic1@gmail.com

have enabled a large degree of networking and the production of an unimaginable amount of data, even in a relatively short period. Along with the mentioned trends, there is a sudden increase in tourist trips and visits to the most distant destinations. All this results in a series of positive changes that enable easier and faster communication with many advantages that have also influenced the development and business of the hotel industry. One part of them is popularly called "travel technologies" and includes various tools and digital platforms that aim to improve guest experiences in the hospitality and travel sectors. These are advanced booking mechanisms, property management systems, customer relationship management software, chatbots based on the application of artificial intelligence, etc. [1]. The application of the aforementioned technologies increases efficiency by providing better insight into user satisfaction, reducing the workload of staff in terms of providing personalized services, as well as automating routine tasks. In addition, these tools enable a high degree of integration with social networks so that their visibility and availability in the sea of information on the Web is very pronounced and of a global character. In a certain way, social networks can significantly contribute to the hotel business, because they provide an additional dimension to the user experience, even before a specific client decides on one of the many alternatives offered.

However, on the other hand, this development of communications and openness brings with it many dangers that come from the cyber world. Therefore, in addition to preventive action, it is necessary to permanently improve numerous types of protection. Undeniably, in the hotel industry as well, all issues of security in cyberspace are becoming topics and actions of local to global importance. The needs of modern people, tourists and guests, are also growing in the virtual world, and they depend on the quality digital services that are offered, they are based on information and communication technologies, which rapidly accelerate the interaction of clients and the services offered.

This paper examines that negative impact of tourist trends, on the hotel business, and the living and social environment. Therefore, security actions are necessary at all times because attackers, more and more often, choose attack methods and techniques rather than targets and timing of cyber attacks. With the appearance of general crises, especially caused by non-economic reasons (pandemics, earthquakes, floods, wars, etc.), attacks on hotels multiply, and the possibilities of endangering hotel guests become not only more frequent but also more reckless. In return, such activities of attackers leave indelible consequences on the satisfaction of tourists but also limit their trips to risky destinations.

Cyber security and the hotel industry

Cyber security is a concept that is not easy to define and determine, due to the complex relationships between the concepts of security and similar concepts, as well as the increasing complexity of the changing unsafe environment in which space is constantly being created for new ways of exploiting the vulnerabilities of computer

systems. A large number of authors equate the terms cyber security, information security and ICT security, which is not necessarily the case. Information security, in its basic form, is represented by three characteristics: confidentiality, integrity and availability [2, pp. 65–66]. If we limit the content of some information to that set of users who have the privilege to see it, while making it impossible for everyone else, then we are talking about confidentiality, which is often called secrecy. Information has integrity if it has not been modified by unauthorized users. Availability refers to the characteristic of information to be available whenever some authorized user requests it. All these features make up the famous "CIA triad" or triangle of information security.

Non-repudiation, accountability, authenticity and reliability are characteristics that expand the notion of the "CIA triad" according to the ISO/IEC 27000:2018 standard, which additionally defines ICT security [3]. Non-repudiation is the property of proving an event that cannot later be disproved. Accountability ensures that the actions of an entity can be uniquely traced back to that entity. Authenticity ensures that an entity is who it claims to be. Reliability is the property of consistent intended behaviour and results.

In his research, von Solm tries to clearly define the concept of cyber security, in such a way as to indicate the differences that exist in the concepts of information security, security of information and communication technologies, abbreviated ICT security and cyber security [4]. The main difference is that cyber security can include assets that are not based on information that are vulnerable to threats through ICT such as digital violence, threats that can arise from the abuse of automated systems such as e.g. smart homes, damages that can be caused by illegal sharing of various digital media and cyber terrorism. NIST defines cybersecurity as preventing damage to, protecting, and restoring computers, electronic communications systems, electronic communications services, wire communications, and electronic communications, including the information contained therein, to ensure their availability, integrity, authentication, confidentiality, and non-repudiation [5]. Cyber security is a complex topic and more and more attention is being paid to it due to the seriousness of the consequences that can be caused by various types of cyber attacks. Concerning the character of the committed act or type, cyber crime can be [6, p. 421]:

a) political - cyber espionage, hacking, cyber sabotage, cyber terrorism, cyber warfare;
b) economic - cyber fraud, hacking, theft of Internet services and time, piracy of software, microchips and databases, cyber industrial espionage, fraud Internet auction - non-delivery of products, false product presentation, false assessment, upgrading product prices, association to achieve higher prices, trade-in black market goods, multiple personalities;
c) production and distribution of illicit and harmful content - child pornography, paedophilia, religious sects, dissemination of racist, Nazi and similar ideas and attitudes, abuse of women and children, manipulation of prohibited products, substances and goods, drugs, human organs, weapons;

d) cyber privacy violations - monitoring e-mail, spam, phishing, eavesdropping, monitoring e-conferences, uploading and analyzing cookies.

The hotel industry is very attractive to cybercriminals, due to the many vulnerabilities that exist and the potential for exploiting these vulnerabilities, usually for financial gain. This is causing great concern for management and they see cybersecurity as a key issue to tackle [7]. The large amount of sensitive data that this type of business collects about its customers, such as personal information about guests' names, residential addresses, email addresses, phone numbers, payment card information, etc., motivates malicious users to attack such systems and unauthorized download and use of that data. The fact that awareness of cyber security and information security culture is at a low level and that the services offered in the hotel business are not necessarily safe also helps them. As the simplest example, we can take the free wireless Internet connection that is offered in hotels and which, as an unwritten rule, the vast majority of guests use. If the wireless network is not adequately protected, the attacker can eavesdrop on the entire traffic of the guest and perform additional analyses, even with free and readily available software such as e.g. packet and protocol analysis software (packet sniffer).

If guests experience inconvenience and become targets of a cyber attack, the consequences will not only be borne by them as individuals, but it can also have a larger scale and destroy the reputation or threaten the reputation of the hotelier. This can additionally trigger a drop in demand for the services offered by a specific hotelier and thus directly threaten its mission, vision and goals. In this context, the hotel industry has a much bigger problem than it may seem at first glance, which is to constantly keep its services at a high level of quality, both traditional ones and all the others that belong to the domain of digital services, which are the assumption modern hotel business.

Additional pressure on the hotel industry was caused by the COVID-19 pandemic, which, in addition to causing problems related to endangering human lives, was followed by a crisis that opened up a series of problems such as unemployment, social distancing, disruptions in business and everyday life [8]. Some authors have pointed out that natural disasters, crises and significant public events create excellent conditions for launching cyber attacks [9], [10, p. 3]. One of the first recorded cases of cyber fraud related to natural disasters occurred back in 2005 after Hurricane Katrina. The FBI conducted an investigation, where it was established that the fraud was carried out in such a way that the attackers sent mass emails, presenting themselves as the Red Cross, to make more expensive donations and humanitarian aid for the vulnerable [11]. When users went to the website shown in the email, they were required to enter information and select the donate option. The fraud was all the more credible because after downloading the data and forwarding it to the attackers, the real website of the humanitarian organization Red Cross was displayed. A recent case in a series of such cyber scams is related to the powerful earthquakes that took place in Turkey and Syria in 2023 [12].

In a global environment that is intertwined with war conflicts, hybrid wars and natural disasters, the hotel business can have significant problems in functioning.

They are further pressed by the need to comprehensively manage their own and their guests' cyber security to maintain their services and reputation at a high level. Therefore, it is very important to identify all the threats that can arise in cyberspace, which can specifically be propagated to the hotel business, and to find an adequate response to them. Some of the most common vulnerabilities that occur in the hotel industry are [13]:

- Card readers / POS terminals - POS terminals facilitate the payment process throughout the hospitality industry but have an increased risk of unauthorized data download. They are suitable not only for processing transactions but also for order and inventory management. The vulnerability of these systems comes from the application running on these systems, especially if organizations are using an unsecured wireless connection. Cybercriminals access this device and gain unauthorized access to customer information, such as payment card numbers. Sometimes they can install special devices in the POS terminals so-called skimmers used to download data.
- hotel wireless connection (Wi-Fi) - clients usually use the wireless connection offered in the hotel. If it is unprotected, hackers can take over the hotel's entire computer network, access clients' devices and phones, and infect a large number of devices with malicious software.
- Internet of Things (IoT) - the hospitality industry uses the innovations available through the use of the Internet of Things to improve the customer experience and make things more efficient. Examples can be: LED lighting that reacts to daylight, interactive screens where guests can download various information about location, weather, etc., locks that use facial recognition to enter a room or room, and smart thermostats that are used for energy efficiency. Each of these smart devices has several vulnerabilities and can be subject to cyber-attacks. Given that the number of such devices is not small, it is necessary to provide all the necessary organizational resources to enable efficient maintenance of such a system, and this can be demanding.
- Hotel websites - Websites have a large number of potential vulnerabilities, where the hotel business provides up-to-date information and enables online reservations. Malicious users conduct cyber attacks to obtain guest data or disrupt regular business operations

Case studies of cyber attacks in the hotel industry

In the last few years, several researches related to the security of the hotel business have appeared. It is evident that a large number of hotels around the world are under the influence of cyber attacks almost every day.

As a first example, we will single out the research published by the company Kaspersky, which refers to the case of RevengeHotels, a targeted cyber campaign carried out employing malicious software (malware) against hotels, hostels, accommodation and travel companies, mainly located in Brazil. It has been confirmed that over 20 hotels targeted are located in eight states of Brazil, as well as in other

countries such as Argentina, Bolivia, Chile, Costa Rica, France, Italy, Mexico, Portugal, Spain, Thailand and Turkey [14]. Bearing in mind that a service was used for shortening links on the Web, such as Bit.ly, it cannot be said with certainty that the targeted campaign was carried out exclusively in the aforementioned countries and it is suspected that its scale is much larger. The main target of the attack is the hotel business using various types of remote trojans (RATs), by cybercriminal groups RevengeHotels and ProcCC, as well as other hackers potentially involved. The campaign has been active since 2015, but its presence has increased during 2019 [15]. The main attack vector was carried out according to a tried-and-tested recipe and included social engineering techniques, such as phishing by creating a virus-infected email attachment in the form of Word, Excel or PDF documents. When the email attachment is opened, custom scripts written in VBS or PowerShell are installed that, without the computer user's knowledge, instruct the user's operating system in the background and download customized versions of various RATs and other malicious software from remote locations, such as is ProCC. In this way, the infected computer can later execute the commands it receives from the remote location. This series of cyber attacks was not created by random attempts and examination of the vulnerability of information and communication infrastructure of hotels and caterers but is part of a designed campaign that used a more advanced version of phishing attacks, spear-phishing. Each email is carefully constructed to make it appear that guests have been contacted by someone pretending to be part of the organization and making a false booking request for a large group of people. It's worth noting that even careful users could be tricked and motivated to open and download attachments from such emails because they contain plenty of details (for example, copies of legal documents and reasons for hotel reservations) and look very convincing. The only detail that can reveal that it is an attack is a small error in the display of the organization's network domain, which indicates that it is a fake domain. The research showed that not only was remote access enabled to the infected computer, but the malware also collected data from hotel reception desks, screenshots, as well as certain customer data and their payment card numbers, as hotel employees often copied documents from OTA (Online Travel Agency) services to charge for services [15]. All the data later ended up on specialized sites on the Web, primarily forums for cybercriminals who made money from the sale of that data and forum subscriptions.
Another example is the cyber attack aimed at InterContinental Hotel Group (IHG), a British multinational company that manages about 6,028 hotels in over 100 different countries in the world, and at the same time has over 1,800 hotels under construction [16]. This multinational company manages the largest hotel chains such as Holiday Inn, Crowne Plaza, Regent, Kimpton, Six Senses, etc. Hackers tried to carry out a ransomware attack and when they failed, they excelled at wiping the data they were accessing. In the initial phase, the attack vector started via phishing and in this way they tricked the employee into downloading the malicious software via an email attachment and in this way they managed to download his code that was used for two-factor authentication. After that, they accessed the most sensitive parts of the IHG system and found the passwords they needed to access the part of the system that

managed the passwords (password vault). The source states that it is completely unexpected that the password that was set is from the category of passwords that are easy to crack. In the concrete example, the password was "Qwerty1234" which is a known password that corresponds to a sequence of letters on the computer keyboard [17] and is recommended not to be used as a password. IHG faced problems and initially did not provide clear information as to whether they were the target of a cyber attack or not, instead they explained that it was website maintenance, only to later come out with a statement that it was an unauthorized access to the system [18]. Due to the timely response of IT staff at IHG, more damage was prevented. However, it is unknown what amount of data was downloaded without authorization, but it is known that for a certain number of employees' accounts, their codes were downloaded. At the time of the attack, and for some time afterwards, the applications and booking systems did not work properly, which caused disruptions in the hotel's operations.

Marriott International Inc. is an American multinational company that includes the hotel chain Marriott Hotels & Resorts, Ritz-Carlton, Le Méridien, Sheraton Hotels and Resorts, Starwood Hotels and Resorts, etc. Marriott International has been the target of many cyber attacks over the past few years, with at least 3 data breaches believed to have taken place. In early 2020, an unauthorized download of data affected up to 5.2 million guests. Before that, Starwood's malware went undetected for 4 years, manipulating millions of data in its reservation system, including credit card and passport numbers. Numerous lawsuits have been brought against Marriott, both by individual guests and by special authorities in the UK, such as the Information Commissioner's Office (ICO). These breaches cost Marriott more than $500 million, plus the company was fined $120 million for GDPR violations [7].

Airlines have a very important place in the value chain that hoteliers create for their customers, together with agencies that organize travel and offer tourist services. If we look at the indirect effects on hoteliers, the problems that can occur with airlines can create the impression that clients can have when they organize arrangements that include air transportation, independently or indirectly through agencies. When we look at cyber security in the hotel industry, we can say that the growing trend of cyber attacks on airlines threatens hoteliers in a certain way. The British Airways case showed that over several hundred thousand user accounts were compromised and a large amount of data was stolen by cybercriminals. Among the compromised data are around 77 thousand payment card numbers, with personal names, account addresses, email addresses, and payment card information including card numbers and CVC values that can be requested during payment. In addition, about 108 thousand payment card numbers were stolen, only without CVC [19]. In the example of MOVEit, it was shown that if there is a vulnerability in the software used, attackers can use it and carry out cyberattacks of greater intensity. This time, British Airways, along with Boots and the BBC experienced an attack that started with a SQL Injection attack, which allowed the cyber group to take control of the database and execute queries through which it could read, write, modify existing and delete data. In the beginning, the cyber attackers decided to download all the data contained in the

databases and forward them to the locations known to them. The data represents the salaries of employees of these three companies listed above and it is estimated that over 100,000 employees were affected by this attack [20]. After that, they contacted the organizations using the MOVEit software and blackmailed them into paying a ransom or making the data publicly available. The group behind Clop ransomware did not directly communicate with the victims of the attack via email, as is usual when it comes to kidnapping (ransom), but via a blog, in which they stated that they accessed the data through the Zellis Payroll software. This situation in which attackers discover flaws in the system before the software manufacturer makes adequate patches to eliminate those flaws is called a zero-day vulnerability. Although the list of victims of the cyber attack has been published [21], its scale is very large and it is not yet fully known which companies have suffered damage.

Protection of hotel business in cyberspace

Cyber security has mitigation of cyber attacks as one of its goals. It is far more realistic to talk about mitigation than to talk about complete prevention because it is about previously researched and analyzed system weaknesses, then well-planned and organized targeted attacks, which are carried out much more often by specialized cyber groups with a clear intention and goal, than by curious individuals who they work in a random way [22]. In addition, for certain types of attacks, such as e.g. DDoS attacks, there is no defence, because cybercriminals use the deep-rooted mechanisms on which the Internet and other networks are based to carry it out. According to some sources in this industry, the following cyber-attacks are the most prevalent [23]:

- related to data or identity theft
- DarkHotel attack
- phishing
- ransomware
- attacks on POS terminals
- DDos attack.

The hotel business has its specifics and it is not easy to propose measures that should be applied to protect them, but we can roughly group them into several categories:

- technical and technological protection measures,
- protection measures related to the impact on people's behaviour when using ICT,
- protection measures resulting from the application of general security principles and their modification to cyberspace.

The complexity of implementing technical and technological protection measures comes from the fact that hotels have a large number of access points in various locations where they are located. The measures should first of all consist of securing and then managing VPN services. Hoteliers should adopt the principle that Internet access for both their employees and guests is achieved through VPN. In this way, an encrypted communication connection is created between the participants in the communication and thus enables the secrecy of all sensitive data that can be sent over the network. Also, it is necessary to properly design and set which rules and

restrictions apply within the organization's network, how to implement the division into subnets what are the rules of communication between subnets, and which rules apply to clients who need to provide free Internet, most often via a wireless connection (Wi-Fi). Considering that POS terminals are often left without physical supervision and this qualifies them as good candidates to which malware can be loaded, it is necessary to deal with the ways of accessing the POS terminal, its operating system, as well as the possibilities of encrypting the data on the POS system itself, because and it realizes client-server communication. In addition, POS terminals should be secured with anti-virus software to prevent the loading of malware. At the same time, the entire POS system should be kept in the internal network and remote access disabled. A large number of attacks begin with the placement of various social engineering techniques in the form of phishing, spearphishing, etc. Potential targets, who come from both sides: from the ranks of hotel employees and service users, should be aware that the Internet is an unsafe place and that they can be part of such an attack at any moment. Cyber attacks that produce more damage, such as e.g. ransomware (blackmail/kidnapping software), are most often distributed to the system after a successfully conducted phishing attack. Hoteliers can organize specialized training for their employees to raise awareness of possible cyber attacks and thereby raise the level of their IT security culture. Basic training of this type consists of the simulation of phishing attacks on employees without their knowledge by specialized IT companies that provide this service, and then direct work by them with employees in order to raise awareness. Raising the level of IT security culture of clients is far more difficult to implement, because it is a global problem, and at the same time, a problem for each country individually. Therefore, normative and strategic documents should be adopted at the international and national levels with the aim of improving the state of cyber security and reducing heterogeneous risks for individuals, organizations and countries [24]. This means that there is a need to incorporate designed programs within each country, through the primary and secondary education systems, in a way that aims to raise the awareness of future users of hotel services about cyber security. What is not sufficiently explained in the literature is the extent to which certain security-specific concepts can be applied to cyber security. It can be assumed that the existence of an objective threat is not necessary for the representation and construction of security, but an attempt to determine it through the process of securitization. It means that securitization should be seen as a means of understanding and the process of construction of what is considered a threat and a collective response to it [25, p. 167]. The basic elements of the securitization concept stand out [26]: securitizing actors, functional actors, speech act, audience and special measures. The audience represents one of the leading objects of constructive criticism in the period after the final establishment of the concept of securitization. It represents those whom the securitizing actors address, and it depends on it whether a securitizing move will be successful and receive the "title" of a successfully implemented securitization, or will remain at the level of a securitizing move. Securitization is formulated as an extremely intersubjective category, following the question of success or failure, as a practical elevation of a certain issue to the security agenda [24]. Some research attempts to

conceptualize securitization in the field of cyber security policies [27]. As the same terms are interpreted differently from the perspective of different scientific disciplines, it can be said that the issue of securitization in cyberspace is a very complex issue that requires consideration from many different aspects and as such is currently in an initial phase and seems to be a candidate for some other researches.

Conclusion

World crises, wars, the COVID-19 pandemic and post-pandemic circumstances are just some of the limiting factors facing the hotel business. Additional pressure is created by cyber attacks, the main goal of which is the unauthorized download of data and information, the subsequent trading of the same on the dark net and obtaining financial benefits. According to some research [28] the hospitality industry, together with retail and wholesale, allocates the least funds for investing in cyber protection. As a product of this, there is an increasing number of cyber-attacks occurring in this domain of business. Currently, the situation is such that the largest entities in the hotel industry, multinational companies, do not invest much in the protection and implementation of certain cyber security policies because the damage that can occur from a cyber attack is much smaller than the profits that these companies make. On the other hand, their attitude towards cyber security is contradictory to their behaviour in that they care a lot about the impression and protection of the reputation they have with their customers because it often happens that they cover up that one or more hotel chains have been the target of cyber attacks and the theft of customer data.

In order to respond to the threats that come from cyberspace, it is necessary to apply technical and technological measures in a complementary manner and to act to change people's behaviour in terms of security and IT culture. In this way, it is possible to prevent potential attackers to a lesser extent, and to a greater extent to mitigate the actions of cybercriminals. The role of the state can help raise awareness of the Internet as an unsafe place and the level of security culture, through the education system, and thus enable users of hotel services to behave consciously and responsibly in relation to cyber threats.

References

[1] D. Elphick, "How travel technology is changing for hotels," 2024. https://www.siteminder.com/r/travel-technology/ (accessed Jun. 23, 2024).

[2] D. Bourgeois, *Information Systems for Business and Beyond*. Saylor Foundation, 2014.

[3] ISO/IEC, "ISO/IEC 27000:2018 - Information technology - Security techniques - Information security management systems - Overview and vocabulary," 2018. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (accessed Apr. 10, 2023).

[4] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.
[5] NIST, "cybersecurity," *NIST Glossary*. https://csrc.nist.gov/glossary/term/cybersecurity (accessed Apr. 10, 2023).
[6] I. Šarenac, "Internet fenomen-Cyber kriminal," in *ICDQM-2017*, 2017, 421.
[7] M. Blanco, "Cyber Security Is Awakening as Key Concern for Hoteliers - Hospitality Makes Attractive Target for Hackers," 2024. https://www.costar.com/article/804855050/cyber-security-is-awakening-as-key-concern-for-hoteliers (accessed Jun. 23, 2024).
[8] S. L. Vesić, "Impact of COVID-19 on Cybersecurity," in *SIGNIFICANCE and treatment of current world trends*, E. Stojić-Karanović and K. Ristić, Eds. Belgrade: International scientific forum "Danube - river of cooperation," 2023, 115–131.
[9] K. Tysiac, "How cybercriminals prey on victims of natural disasters," *Journal of Accountancy*, 2018. https://www.journalofaccountancy.com/news/2018/sep/cyber-criminals-prey-on-natural-disaster-victims-201819720.html (accessed Apr. 10, 2023).
[10] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Comput. Secur.*, vol. 105, 2021, doi: 10.1016/j.cose.2021.102248.
[11] B. Ross and J. Rackmill, "Katrina Internet Charity Scams Try to Dupe Donors." https://abcnews.go.com/Blotter/HurricaneKatrina/story?id=1106006&page=1 (accessed Apr. 10, 2023).
[12] A. BÎZGĂ, "Cybercriminals exploit human misery in earthquake-hit Turkey and Syria with new online disaster scam," 2023. https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-exploit-human-misery-in-earthquake-hit-turkey-and-syria-with-new-online-disaster-scam/ (accessed Apr. 10, 2023).
[13] K. Chin, "Cybersecurity in the Hospitality Industry: Challenges and Solutions," 2023. https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry (accessed Jun. 23, 2024).
[14] SECURELIST, "RevengeHotels: cybercrime targeting hotel front desks worldwide," 2019. https://securelist.com/revengehotels/95229/ (accessed Jun. 23, 2024).
[15] Kaspersky, "Not-so-safe travels: cybercriminals stealing guests' credit card data from hotel front desks worldwide," 2019. https://www.kaspersky.com/about/press-releases/2019_not-so-safe-travels-sybercriminals-stealing-guests-credit-card-data-from-hotel-front-desks-worldwide (accessed Jun. 23, 2024).
[16] N. Foster, "IHG (InterContinental Hotel Group) Cyberattack," 2023. https://www.acecloudhosting.com/blog/ihg-cyberattack-2022/ (accessed Jun. 23, 2024).
[17] A. Mascellino, "Hackers Admit Destroying InterContinental Hotels Group's Data 'For Fun,'" 2022. https://www.infosecurity-magazine.com/news/hackers-destroying-ihgs-data-for/ (accessed Jun. 23, 2024).
[18] InterContinental Hotels Group PLC, "Unauthorised access to technology systems," 2022. https://www.londonstockexchange.com/news-article/IHG/unauthorised-access-to-technology-systems/15617013 (accessed Jun. 23, 2024).

[19] Gibraltar Chronicle, "British Airways admits 185,000 more customers compromised in cyber attack," 2018. https://www.chronicle.gi/british-airways-admits-185000-more-customers-compromised-in-cyber-attack/ (accessed Jun. 23, 2024).
[20] J. Tidy, "BBC, BA and Boots issued with ultimatum by cyber gang Clop," 2023. https://www.bbc.com/news/technology-65829726 (accessed Jun. 23, 2023).
[21] N. Goud, "List of victimized companies of MOVEit Cyber Attack." https://www.cybersecurity-insiders.com/list-of-victimized-companies-of-moveit-cyber-attack/ (accessed Jun. 23, 2023).
[22] S. L. Vesić and M. Bjelajac, "CYBER SECURITY OF A CRITICAL INFRASTRUCTURE," *Pravo - Teor. I Praksa*, vol. 40, no. 2, 77–88, 2023, doi: 10.5937/ptp2302077V.
[23] Social Tables, "Cybersecurity for Hotels: 6 Threats Just Around the Corner from Your Property." https://www.socialtables.com/blog/hospitality/cyber-security-hotels/ (accessed Jun. 23, 2024).
[24] D. Vesić, J. Sánchez Monroe, and S. L. Vesić, "Cyber security and protection against high-tech crime," in *SETI IV - Fourth International Scientific Conference - SCIENCE, EDUCATION, TECHNOLOGY AND INNOVATION*, 2022, 91–98.
[25] B. Buzan, O. Wæver, and J. de Wilde, *Security: A New Framework for Analysis*, 1st ed. Lynne Rienner Pub, 1997.
[26] M. Gnjatović, "Primena koncepta frejminga u sekuritizaciji sajber pretnji," *Godišnjak Fak. bezbednosti*, vol. 1, 153–168, 2018, doi: 10.5937/GFB1801153G.
[27] M. Górka, "Conceptualising securitisation in the field of cyber security policy," *J. Mod. Sci.*, vol. 53, no. 4, 263–290, 2023, doi: 10.13166/jms/176103.
[28] Hotel technology news, "With Disruption of Booking Channels, InterContinental Hotels Group Becomes the Latest Cyberattack Target," 2022. https://hoteltechnologynews.com/2022/09/with-disruption-of-booking-channels-intercontinental-hotels-group-becomes-the-latest-cyberattack-target/ (accessed Jun. 23, 2024).