smart cities

MDPI

Article

The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities

Lázaro Florido-Benítez

Department of Economics and Business Administration, University of Málaga, 29016 Málaga, Spain; lfb@uma.es

Abstract: The purpose of this paper is to analyse the cybersecurity in online travel agencies (OTAs) and hotel sectors to protect users' private data in smart cities. Methodologically, this research uses a sample of information about cyberattacks that occurred during the period of 2000–2023 in companies operating as OTAs and in the travel, tourism, and food sectors, which was obtained from research articles. Then, we had to expand the research to include updated information about cyberattacks from digital newspapers, regulatory sources, and state data breach notification sites like CSIS, KonBriefing, EUROCONTROL, and GlobalData. The findings of the current research prove that hotels and OTAs were constantly exposed to cyberattacks in the period analysed, especially by data breaches and malware attacks; in fact, this is the main novelty of this research. In addition, these incidents were severe for both guests and tourism companies because their vulnerabilities and consequences affect the reputation of companies and smart cities where these firms operate, as well as consumer confidence. The results also showed that most of the cyberattacks examined in this manuscript were aimed at stealing information about the companies' and users' private data such as email addresses; credit card numbers, security codes, and expiration dates; and encoded magstripe data; among many other types of data. Cyberattacks and cyberthreats never disappear completely in the travel and tourism sectors because these illegal activities are closely related to the hacker's thirst for power, fame, and wealth.

Keywords: cybersecurity; cyberattacks; OTAs; hotels; consumer; smart cities; tourism industry

Citation: Florido-Benítez, L. The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities. *Smart Cities* **2024**, *7*, 475–495. https://doi.org/10.3390/smartcities7010019

Academic Editor: Pierluigi Siano

Received: 6 January 2024
Revised: 1 February 2024
Accepted: 2 February 2024
Published: 4 February 2024

1. Introduction

E-commerce in the tourism industry is a virtual scenario where consumers, sellers, and dealers meet without the need for physical contact [1]. This digital scenario requires one to be protected against cyberthreats, cyberattacks, hackers, cybercriminals, hacktivists, or even foreign countries traditionally seen as opponents trying to find and exploit existing vulnerabilities in public and private tourism companies. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks, and it must be implemented in all travel and tourism companies to tackle the new challenges of digital tourism activities. Cybersecurity means protecting companies, cities, governments, and consumers from cyberthreats like phishing, identity thefts, ransomware, data breaches, and internet fraud, among many other activities [2]. In the case of online travel agencies (OTAs), a cyberattack by a hacker or cybercriminal is substantially detrimental to the firm's reputation and customer trust, and this incident has severe financial, legal, and regulatory implications [3]. For instance, Orbitz, a subsidiary of the online travel agency Expedia, reported that hackers accessed personal information from about 880,000 payment cards.

The issue is that the OTAs' incomes pivot around the commission of products and services provided and sold by different suppliers such as airlines, hotels, car rental companies, or travel insurance firms, and this makes it difficult to find potential threats and

vulnerabilities. In OTAs' websites and apps, the reality is more complex than that, given that it implies firms do not properly and continuously evaluate all suppliers of services in the supply chain and operational processes with their customers [4]. This is due to a lack of interoperability and information between businesses and consumers [5], allowing for an ideal environment for hackers and cybercriminals. There are great vulnerabilities in the tourism supply chain seen from the supply and demand side after the pandemic crisis [6]. OTA users' two main concerns are privacy and security barriers when they use OTAs' web and app platforms [7] because they perceive their personal information as being exposed to possible cyberattacks [8].

However, OTAs' and hotels' vulnerabilities directly influence tourists' experiences in the smart cities where they are located. We cannot forget that smart cities are socio-technical platforms that interact with residents, tourists, and companies. Therefore, cybersecurity must be implemented in companies, people, government policies, and smart cities to ensure commercial and private transactions. Cybersecurity protocols enhance consumers' privacy and security in smart cities and make them more aware when their data are used by travel and tourism firms [9]. It is very important to emphasise that there are no 100 per cent safe spaces; the risk of a cyberattack is always latent [10]. There is a lack of research on the protection systems against cyberthreats in smart cities [9,11,12]. Most modern cities are striving to become smart cities; for this reason, they are implementing better cybersecurity protocols to prevent cyberthreats [13].

Security vulnerabilities present in cybersecurity systems cause firm- and user-level security issues. The tourism industry's world is conditioned by digital technology [14], and cyberthreats, in view of the information, data, and digital operations, constitute a significant risk factor for businesses. The relationship between e-commerce and cybersecurity is viewed with great concern by OTAs, hotels, smart cities, and users in security, privacy, and economic terms. The COVID-19 pandemic has led to the accelerated implementation of new processes and services in the e-commerce tourism sector that require new security and privacy measures, but such efforts will be not easy to make visible to the consumers [15,16]. As businesses and users increase information sharing via the internet, the vulnerability to attack rises. Chen and Fiscus [17] found that the increasing frequency of data breach incidents in the last ten years indicates that the issue of cybercrimes has become more critical in the hospitality industry. In 2022, digital fraud attempts rose by 156% in the travel and leisure sectors; in fact, the Marriot International and InterContinental Hotels group booking apps have fallen victim to hackers [18].

OTA and hotel payment processing and online reservation systems contain enormous amounts of customer credit card and private information. Breaches to these systems allow hackers to access cardholders' information and personal identities [19]. There are limited studies in the context of the cybersecurity applied by OTAs, hotels, smart cities, and user context as a topic [20]. Several studies have made efforts to examine cybersecurity in the hospitality industry [17], technology and transportation sectors [21], and food industry [22]; data breaches in the hotel industry [23]; communication and information in the hotel industry [24]; digital wallets [25]; the Internet of Things (IoT) [26]; consumer's trust in OTAs [27]; cybersecurity threats in the e-commerce sector [28]; or even cyberattacks on the hospitality sector [29].

More attention should be devoted to cybersecurity in OTA, hotel, and smart city studies [30,31]. Indeed, there are no studies that tackle the cybersecurity of OTAs, hotels, smart cities, and consumers. To fill this knowledge gap, the purpose of this paper is to analyse cybersecurity used in the OTA and hotel sectors to protect users' private data in smart cities. The results of this research will help OTA operators, hotel operators, and smart city managers to understand the new challenges of cybersecurity, cyberthreats, and cyberattacks that they face daily, and to admit that hackers and cybercriminals are always one step ahead. Morrison and Buhalis [14] note that the sharing economy disrupts the marketplace and brings both benefits and disadvantages to service ecosystems.

2. Literature Review

The tourism industry holds hugely valuable and sensitive data on every traveller. Travel and hospitality companies must remain vigilant to prevent future cyberthreats and cyberattacks in an evolving cybercrime landscape. In addition, as the digital ecosystems of travel and tourism companies grow, they become more vulnerable to cyberattacks. Hackers exploit the vulnerabilities within a cybersecurity strategy, so a rigorous approach is central to effective risk management [6]. To tackle cyberthreats, a company's cybersecurity strategy must involve contingency planning, outlining immediate actions, post-breach responses, and an understanding of the organisation's current cyber risks [10]. For instance, a data breach can destroy an OTA or hotel business due to a loss in reputation, business disruption, the cost of remediation after a cyberattack, regulatory costs, and lawsuits [32]. From the customer's point of view, a cyberattack can lock guests out of their rooms, forcing them to make reservations elsewhere [32].

2.1. The Cybersecurity in the Context of OTAs, Hotels, and Smart Cities to Enhance the Sensitivity and Private Data of Users

The expansion and internationalisation of companies through e-commerce have provided an incentive for attacks by cybercriminals, hackers, hacktivists, and foreign countries. Online shoppers need to be confident that their data and personal information are protected by online firms against hackers and cybercriminals firms [33]. Nevertheless, it is important to stage a taxonomy of the concept of cybersecurity and the types of cyberattacks in OTA and hospitality industries, which will help to identify the main differences in each type of cyberattack. The concept of cybersecurity is defined as a set of technologies and processes designed to protect computers, networks, programs and data from attack, damage, or unauthorised access [34].

The act of protecting information and communication technology (ICT) systems using software programs, good practices, and training levels of employees from cyberthreats and cyberattacks is known as cybersecurity [10,35]. The probability of suffering a cyberattack is mainly determined by a firm's degree of digitalization [36]. For instance, smart cities should create more efficient cybersecurity protocols and practices to protect citizens' and tourists' privacy data and the commercial activities of companies [9]. Indeed, Demertzi et al. [37] note that the growth of the Internet of Things (IoT), augmented reality (AR), artificial intelligence (AI) extended reality (XR), and virtual reality (VR) digital tools provide new vulnerabilities and cyberthreats at smart cities and companies. The investment in cybersecurity is related to the capabilities of smart cities and companies to resolve/anticipate/protect themselves against future threats and attacks, and to guarantee the operability of their communication and information systems [38].

From the standpoint of users and workers, the degree of responsibility and understanding of users to protect an organisation's data and networks against possible vulnerabilities and threats is defined as "cybersecurity awareness" [39]. Therefore, companies and users should know what types of cyberattacks exist in the travel and tourism sectors, as well as be able to identify them if they occur to protect their private information. The ubiquity of information and big data (in terms of users) are crucial for OTA and hospitality sectors in order to make better marketing decisions [40,41]. OTA platforms such as Booking, Expedia, Airbnb, and TripAdvisor signed a data-sharing deal with the European Union (EU) because the General Data Protection Regulation (GDPR) has a significant impact on international data flows to transfer personal data between countries [42,43]. In Europe, companies are legally obligated to inform the Information Commissioner's Office (ICO) if they suffer a cyberattack that involves the personal information of customers or employees. In the case of U.S. companies, they must report a cyberattack to the FBI's Internal Crime Complaint Center (IC3)

The sensitivity of the private data of users by public and private organisations may be compromised by cyberattacks; for this reason, it is very important to implement

cybersecurity protocols by public and private organisations. Indeed, the lack of control of users' data by companies and the vulnerabilities regarding private data disclosure in terms of data breaches have harmful legal and economic consequences [44,45]. For OTA and hotel firms to implement appropriate management and cybersecurity technology tools such as mobile apps, social media, VR, AI, big data, VeraCrypt, Argo UML, CipherShed, Anaconda Python, Eclipse, Hadoop, and information systems, it is required that managers and staff are familiar with these different types of tools to prevent possible vulnerabilities and future cyberattacks [31,46]. When consumers log onto a website or app or use a search engine, they are aware that their preferences for privacy are often disregarded by the advertising industry and regulators [47]. A solution for OTAs, hotel operators, and marketers to respect consumers' privacy expectations is enhancing critical transparency and avoiding the exploitation of individual vulnerabilities to improve consumers' experiences and security [48,49].

2.2. The Types of Cyberattacks in the Tourism Industry

Information technologies prevail in all functions of strategic and operational management of the tourism industry [50]. Assessing how travel and tourism companies such as tour operators, OTAs, and DMOs are utilizing cybersecurity to drive revenues will help understand organisations and researchers the latest cybersecurity trends within the travel and tourism landscape [51,52]. Users' sensitive data must be protected by organisations to avoid significant risks for customers due to hackers. In 2022, the global average number of cyberattacks against organisations in the tourism and leisure sector increased by 60% in comparison with 2021 [53]. In 2018, a data breach impacted 500,000 British Airways customers. The data breach compromised login, card payment, and travel booking details, while credit card details were being stolen as they were being entered [54]. For example, Málaga, Barcelona, Singapore, and London smart cities assess their governance models and their cybersecurity measures to prevent possible cyberterrorism and cyberthreat activities [11]. Cyberattacks on smart cities could generate significant damage, including the shutdown or compromising of vital services such as electricity, water, and transportation [55].

Attackers look for vulnerabilities in the systems to launch different kinds of network attacks. For this reason, the construction of a tourism database is needed to guarantee the safety of a user's personal information and to protect it against cyberattacks [56]. With the aim of considering the effects of exposure to cyberattacks in the tourism industry, Table 1 presents the types of cyberattacks supported by expert authors to better understand the difference between them. In the travel and hospitality sectors, applications and systems are exposed to the internet and entry points for users; therefore, these sectors are more exposed to cyberattacks that collect personally identifiable information, credit card details, and other sensitive information stored in travel and hotel firms [57,58]. Prabhu et al. [59] found that the current measures hotels and OTAs take to ward off cyberattacks are inadequate and dated, and most of their employees lack the knowledge to deal with them [36,60,61].

As stated by Wynn [62], there is a lack of communication and interoperability between smart cities and companies, generating a high vulnerability and integrity of users' private data and cybersecurity protocols. That is precisely why the resilience of smart cities and companies lies in the ability to rapidly adapt and respond to internal or external changes and continue operations daily against possible cyberattacks. Cyberattacks and cyberthreats directly impact the companies' cybersecurity risk maturity and their business portfolio [63]. It would be important to use a behavioural approach in recognizing problems and the need to increase public knowledge and awareness of the application of cybersecurity in the travel and tourism sectors, in order to educate people about the importance of cybersecurity when they are buying or booking products and services in e-commerce firms. For instance, Botnet attacks on hotels can cascade into an urban operating system that then cascades into other systems, such as water and electricity

management or emergency response. In smart cities, systems are linked together to manage city services, and this digital synergy is one of the key security risks in a smart city [64].

Table 1. Types of cyberattacks in the travel and tourism industries.

Type of Cyberattacks	Definition	References
Phishing	It is used to obtain sensitive information from users, such as online banking login credentials, company login credentials, credit card details, login credentials, or passwords.	Alawida et al. [21]
Ransomware	The goal of this attack is to deny its owner or user access to it, and after that, the user pays the attacker directly. The ransomware is programmed to identify the organisation's most sensitive or valuable data.	Sheridan [65]
DDoS	It is a type of cyberattack in which cybercriminals aim to crash a computer system or server, making sites and services unavailable to customers. These attacks are commonly used by hacker groups to force websites to go offline.	Chaganti et al. [66]
Botnets	Botnet attacks use networks of thousands of computers for malicious login attempts, mass spam attacks, or takedown of a network, network devices, and websites.	Elliot [67]
Data breach	It is a data breach that exposes confidential, sensitive, or protected information to an unauthorised person.	Schlackl et al. [68]
Password attack	A password attack is used to exploit the authentication of user accounts. Password attacks involve exploiting a broken authorisation vulnerability in the system combined with automatic password attack tools that speed up the guessing and cracking of passwords.	Al-Shareeda et al. [69]
Hacking	Hacking involves forcefully gaining unauthorised access to it, such as by disabling the security measures of a computer network.	Muñoz et al. [70]
Website/app breach	A website or app attack is a cyber assault in which sensitive, confidential, or otherwise protected data are accessed and released illegally.	Ukwandu et al. [71]
Insider	An insider is someone who commits illegal activity against her/his own firm.	Smith and Rupp [72]
Man-in-the-Middle	An attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.	Huang et al. [73]
Human error	It refers to an employee either doing something he should not or failing to do something he should. Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems.	Le Coze [74]
SQL injection	It is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.	Alawida et al. [21]
Point-of-sale (POS)	Point-of-sale (POS) attacks give hackers valuable data including credit card information such as card numbers and personal identification numbers (PINs).	Paraskevas [3]
Zero-day exploit	Zero day gets its name from the number of days that a patch has existed for the flaw "zero". It is a cyberattack that takes advantage of a zero-day vulnerability to install different types of malwares, steal sensitive data or credit card numbers, and cause data breaches.	Deshpande et al. [75]

Companies' vulnerabilities come about from their dependence on ICT systems, and a cyberthreat in the ICT system can come from a source internal or external to the company that can cause economic, social, political, and operational implications [10,76]. In 2021, one of the largest cyberattacks in U.S. history happened, and over 60 thousand companies worldwide were affected in terms of privacy and safety. Hackers took advantage

of a few coding errors and four different zero-day vulnerabilities that allowed them to take control of Microsoft's systems. They had unauthorised access to emails from firms to local governments, and only needed two conditions to break into each individual company's email servers: connection internet and on-premises (locally managed systems). Microsoft and the Federal Bureau of Investigation (FBI) accused China of the data breach [77]. In 2022, Microsoft was hacked again by the so-called Lapsus$ hackers; this group used social engineering to hijack an account and gain access to Microsoft's system. Digital trust is defined by ISACA [78] as the confidence in the relationship and transactions among providers and consumers within the digital ecosystem. Overall, 95% of cybersecurity breaches are caused by human error, so it is important that consumers trust the humans behind the businesses they interact with to protect their information [78].

2.3. The Perspective of the Consumer against Present and Future Cyberattacks

OTA and hotel websites and apps must provide users with a positive user experience and security in business-to-consumer (B2C) terms, as their primary goal is to draw a visitor into completing an online purchase. Indeed, user experience and security are key factors for e-commerce activity [79]. In 2010, the International Organization for Standardization (ISO) defined the user experience as "a person's perceptions and responses that result from the use and/or anticipated use of a product, system, or service" [80]. User experience is a person's perceptions of usability, security, satisfaction, and the interaction between products and services provided by companies through websites and apps [81]. The interest of consumers in safety and security measures is directly proportional to the level of the company's prestige or hotel classification [82]. Thousands of cyberattacks are launched every day against internet users across the world, and companies and governments need to prevent these attacks to ensure the security private data of users. In 2020, the number of cyberattacks increased by over five times (530%) in the European aviation industry [83].

OTAs and hotels are striving to improve user experience and security to retain more customers. The relevance of OTAs in e-commerce and their strategic position in the tourism market has motivated large B2C companies like Google, Baidu, Tencent, and Alibaba to invest in their own OTA websites [84]. OTA and hotel operators need to provide refund policies and security-alert messages to users in the case that they suffer cyberattacks to raise their operational transparency because these good practices will help to enhance users' experience and security [85]. When customers book services online on website and app platforms, they consider the experience and security in their future shopping intention. Promoting the security of transactions and private data using websites and apps helps to extend interactive communication between customers and companies [86]. Users' browsing behaviours on a hotel website differ in terms of the veracity of the information and privacy [87].

OTA and hotel website's security and privacy systems are paramount to improving customers' confidence and their willingness to complete online transactions. Consequently, the security/privacy dimension is defined as the degree to which a customer believes that using the website will be free from danger and risk [88]. The lack of security as perceived by online consumers is one of the main obstacles to the development of e-commerce in the travel and tourism industries [89]. For instance, when consumers use a payment method to buy products and services through websites and apps, they require the confidentiality of the transactions and security of their personal information. OTA and hotel operators need to improve and ensure CRM services and the security of the private data of users to preserve data confidentiality from potential cyberthreats and cyberattacks [90].

2.4. Smart Cities' Need to Prevent Future Cyberattacks and Cyberthreats

In this study, a smart city is one that uses the power of digital technology, data analysis, cybersecurity, AI, VR, AR, and IoT sensors to improve residents' quality of life and tourists' experiences while managing resources efficiently and sustainably to guarantee

the sustainability of the environment and tourism industry in a city. The concept of a smart city is based on the extensive multidimensional use of information and communication technologies to create the most favourable living conditions for residents and visitors [13]. A smart city must provide innovative services in transportation, energy management, and healthcare on a large scale, creating a technologically advanced urban environment that is supported by cybersecurity systems [91]. Overall, 56% of the world's population lives in cities, and this percentage is projected to rise to more than 66% by 2050 [92]. We must be aware that more than 46 million signals of potential cyberattacks are seen on average every single day across the world [93]. For instance, Barcik et al. [94] suggest that smart cities and military technologies must be developed in mutual compliance to assure interoperability and the protection of the population in a city.

The successful development of the smart city of Zurich in recent years has been aided by a sound economic climate, good governance, cybersecurity systems, and the implementation of important technology strategies within the city [95]. In the case of Málaga smart city, cybersecurity is a priority in the management of the governance, tourism, safety, logistics, and air transport activities, thanks to Google's cybersecurity centre, which improved cybersecurity protocols and systems in the entire city [96]. Governance in smart cities involves the gathering, processing, and sharing of intelligence data, which allows smart cities to increase their resilience against future attacks [10,97].

When an airline/OTA/hotel reservation online service has been hacked by cybercriminals, hackers, or hacktivists, this incident has immediate costs and effects on smart cities and their tourism activities. In 2020, EasyJet admitted that the personal details of 9 million customers and the financial data of over 2000 passengers were accessed in a sophisticated cyberattack. Due to this negligence in handling customer data, EasyJet must pay compensation of up to GBP 2000 to each client [98]. Nevertheless, EasyJet's problem does not end here, cybercriminals may open new bank accounts, access the existing ones, make purchases, or commit wrongdoings using stolen users' identities in smart cities, seriously affecting smart cities' brand image and their tourism activities. A smart city is a single system of systems instead of separate independent systems, in order to boost the interoperability between public administration and private organisations, as well as to improve citizens' well-being and quality of life and tourists' experiences [99]. For this reason, blockchain, big data, and AI algorithms are emerging as solutions offering the data security and confidentiality essential for strengthening the security of smart cities [91,100].

3. Methodology

Methodologically, this research uses a sample of information on cyberattacks that occurred during the period of 2000–2023 in companies operating in the OTA, travel, tourism, and food sectors that was obtained from research articles. The tourism industry involves a wide range of businesses [76]. Then, we expanded the research to include updated information on cyberattacks from digital newspapers, regulatory sources, and state data breach notification sites like CSIS [101], KonBriefing [102], Eurocontrol [83], GlobalData [52], AAG [103], among others, to stage the true extent of the cyberattack problems in travel and tourism industries. This methodology has also been used by authors such as Alawida et al. [21], Tong et al. [23], Ukwandu et al. [71], Florido-Benítez [10], Fragniere and Yagci [24], and Arcuri et al. [29]. The method was used to search various databases for papers connected to cyberattack topics, including Science Direct, Elsevier, Emerald insight, IEEE, Springer, Willey, and the Web of Science (WoS) database between 2000 and 2023. This study aimed to analyse the types of cyberattacks faced by travel and tourism companies (see Tables 1 and 2) in the period analysed. It must be noted that this research does not address internal errors in electronic processing, software bugs, or VeraCrypt, Hadoop, VirtualBox, Eclipse, Argo UML, or Anaconda Python programming environments used by cybersecurity experts and computer engineers. This study pinpoints escalating cybersecurity concerns in the context of the tourism industry from a global perspective.

Table 2. Timeline of cyberattacks related to the travel and tourism industries (2000–2023). Source: adapted from CSIS [101], KonBriefing [102], Eurocontrol [83], and Florido-Benítez [10].

Year	Class	Incident Attack	Sector	Country	The Cyberattack Description
2000	Confidentiality	Data breach	Airline	U.K.	EasyJet airlines reported that it had fallen victim to a very sophisticated cyberattack. The hackers gained access to the email addresses and travel information of about 9 million customers.
2008	Availability	Bot	Hotel	U.S.	Wyndham hotels suffered three data security attacks, which resulted in nearly USD 11 million in identity fraud damages.
2010	Confidentiality	DDoS	Hotel	U.S.	HEI Hotels & Resorts were hit by a DDoS attack, exposing the credit card number, expiration date, security code, and encoded magstripe data.
2014	Confidentiality	Malware	Hotel	U.S.	White Lodging Hotels were hacked by malware.
2014	Availability	Ransomware	Hotel	U.S.	The Houstonian Hotel, Club & Spa suffered a ransomware attack that exposed users' credit card information.
2015	Confidentiality	Malware	Hotel	China	For Mandarin Oriental, the Hotel Group reported that Mandarin's credit card system was compromised by a malware attack.
2015	Confidentiality	Data breach	OTA	Germany	Thousands of travel agents in Germany were embroiled in a scandal involving the sharing of sensitive business data by their consortium's head office. The scandal, exposed by business newspaper Handelsblatt, caused uproar in German trade after the leading agency consortium RTK passed detailed sales figures of up to 4000 travel agencies to the tour operator FTI over a period of up to eight years. FTI is Germany's third-biggest operator.
2015	Confidentiality	Malware	Hotel	U.S.	Noble House Hotels & Resorts reported that a malware downloaded guest information from the magnetic strip of credit cards swiped at the subject location.
2015	Confidentiality	Malware	Hotel	U.S.	Starwood Hotels & Resorts were attacked by malware, which stole users' credit and debit card data.
2015	Confidentiality	Malware	Hotel	U.S.	Las Vegas Resort reported that a malware attack collected hotel guests' names, card numbers, and expiration dates,
2015	Confidentiality	Malware	Hotel	U.S.	HEI Hotels & Resorts informed that a malware attack collected the personal information of its guests such as names, payment card numbers, and verification codes.
2015	Confidentiality	Data breach	Hotel	U.S.	BBC News reported that Hilton was fined USD 700,000 for mishandling data breaches in 2014 and 2015.
2016	Confidentiality	Data breach	Hotel	U.S.	InterContinental Hotel Group reported a credit card breach across some 5000 hotels worldwide.

2016	Availability	Hacking	Hotel	U.S.	KrebsonSecurity reported that hackers breached credit card systems at some of the Trump Hotel Collection establishments.
2016	Confidentiality	Malware	Restaurant	U.S.	Landry's, Inc. revealed that hackers installed malware on payment card processing devices that lifted the data from the magnetic swipe stripe of payment cards in more than 300 of the chain's restaurants, hotels, and casinos.
2016	Confidentiality	Data breach	Hotel	U.S.	Millennium Hotels & Resorts North America reported a data security collected customers' card payments.
2016	Confidentiality	Malware	Hotel	U.S.	Omni Hotels reported that a malware attack collected more than 50,000 customer credit and debit cards that had been exposed to the attack.
2017	Confidentiality	Data breach	Travel reservation system	U.S.	Sabre Corporation was hacked by a data breach, and this collected consumers' payment card data and personally identifiable information.
2017	Confidentiality	Data breach	Hotel	U.S.	Hyatt Hotels & Resorts were affected by a data breach into guest payment card information at 41 corporate-managed properties across 11 countries.
2017	Integrity	Hacking	OTA	U.S.	Orbitz, a subsidiary of online travel agency Expedia, reported that hackers accessed personal information from about 880,000 payment cards.
2018	Availability	Data breach	Hotel	U.S.	In March 2019, Marriott company announced that the 2018 data breach cost the company, pre-tax, a total of USD 28 million.
2018	Confidentiality	Data breach	Airline	Hong Kong	Cathay Pacific Airways revealed a data breach that compromised 9.4 million passenger records.
2018	Confidentiality	Data breach	Airline	U.K.	A data breach impacted 500,000 British Airways customers. The data breach compromised login, payment card, and travel booking details, while credit card details were stolen as they were being entered.
2018	Confidentiality	Data breach	Airline	U.S.	Delta airlines confirmed a breach of customer payment details due to a cyberattack. Hackers had unauthorised access to credit card information of fewer than 100,000 of its customers.
2018	Confidentiality	Data breach	Airline	Canada	Air Canada reported a mobile app data breach affecting the personal data of 20,000 people.
2018	Confidentiality	Malware	OTA	France	FastBooking was hit by a malware attack, which collected users' payment card details from guests at hundreds of hotels.
2018	Confidentiality	Data breach	Hotel	China	A breach of data at Huazhu Hotels Group affected 130 million customers and their cell phone numbers, login credentials, addresses, dates of birth, credit card numbers, bank account numbers, and booking details.
2018	Confidentiality	Data breach	Hotel	U.S.	Radisson Hotel Group identified a security breach of data, and this stole users' email addresses and phone numbers.

2019	Confidentiality	Phishing	Hotel	U.S.	Drury Hotels were hit by phishing attacks.
2019	Confidentiality	Data breach	Hotel	U.S.	Choice Hotels International reported a data breach that compromised users' email addresses and credit card details.
2019	Confidentiality	Data breach	Hotel	U.S.	MGM Resorts International suffered a data breach in 2019 that affected 10.6 million guests.
2020	Confidentiality	Data breach	OTA	Spain	A Barcelona, Spain-based software firm called Prestige Software was caught exposing sensitive, private, and financial data of millions of customers around the globe. Customers from Booking.com, Expedia, Agoda, Amadeus, Hotels.com, Hotelbeds, Omnibees, Sabre, and several others are among the unsuspected victims of the data breach.
2020	Confidentiality	Data breach	OTA	U.S.	An internal leak exposed Airbnb hosts' personally identifiable information to other users due to a data breach.
2020	Availability	Hacking	OTA	U.S.	The U.S. travel management firm CWT reported that they paid USD 4.5 million hackers who stole reams of sensitive corporate files and said they had knocked 30,000 computers offline.
2021	Integrity	POS	Restaurant	U.S.	Four restaurant chains in the U.S. disclosed payment card theft via PoS malware that took place over the summer.
2021	Confidentiality	Human error	Supermarket	U.S.	Wegmans Food Markets notified customers that some of their information was exposed after the company became aware that two of its databases were publicly accessible on the internet because of a configuration issue.
2021	Confidentiality	Ransomware	Supermarket	Netherlands	A ransomware attack against warehousing and transportation provider Bakker Logistics caused a cheese shortage in Dutch supermarkets.
2021	Confidentiality	Data breach	Bus transport	U.K.	Nottingham City Transport: Bus operator was hit by a data breach.
2021	Availability	Hacking	Entertainment	Switzerland	The Berlin Zoological Garden announced that one of its external service providers, Ticketcounter B.V., suffered a data breach affecting around 400,000 of its visitors.
2021	Confidentiality	Ransomware	Entertainment	Australia	A Tasmania casino operator suspended operations for 10 days due to a cyberattack that impacted its pokies machines and hotel bookings system for more than a week.
2021	Confidentiality	Ransomware	Hotel	Spain	Meliá Hotels International were hacked by a ransomware attack.
2021	Confidentiality	Website/app breach	Marketing	Hong Kong	Hong Kong marketing firm Fimmick was hit by a cyberattack, according to a British cybersecurity firm monitoring the situation. Fimmick serves several clients like McDonald's, Coca-Cola, Shell, Asus, and others.
2021	Confidentiality	Website/app breach	Supermarket	U.K.	Tesco's website and app was crashed after a web and app breach attack.

2021	Confidentiality	Zero-day exploit	Technology	U.S.	Hackers took control of Microsoft's vulnerable systems due to a zero-day exploit attack.
2022	Confidentiality	Phishing	OTA	Netherlands	Booking.com suffered several cyberattacks on the professional interfaces of hoteliers and their clients.
2022	Confidentiality	Data breach	OTA	U.S.	SevenRooms suffered a data breach.
2022	Confidentiality	Data breach	Hotel	U.S.	The Holiday Inn owner, Intercontinental Hotels Group, confirmed that the company was hit by a data breach attack.
2022	Confidentiality	Data breach	Bus transport	U.K.	Go-Ahead Group confirmed a cyberattack after finding "unauthorised activity" within its IT systems.
2022	Confidentiality	Data breach	Airline	U.S.	American Airlines reported a data breach in which hackers compromised an undisclosed number of email accounts belonging to its personnel and gained access to confidential personal information.
2022	Confidentiality	DDoS	Airport	Taiwan	DDoS attacks targeted Taiwanese websites just before House of Representatives Speaker Nancy Pelosi arrived in Taiwan. At least four websites were targeted, including Taiwan Taoyuan International airport.
2022	Availability	Hacking	Airline	France	Air France—KLM shut down the booking facility on its AgentConnect travel agent portal due to hacking attacks. The airline reported that several OTAs on the French market were affected by cyberattacks.
2023	Confidentiality	Data breach	Airport	Germany	The official websites of Berlin (BER), Frankfurt (FRA), Munich (MUC), Düsseldorf (DUS), Nuremberg (NUE), and Dortmund (DTM) airports fell victim to large-scale DDoS attacks, and this caused the websites of the airports to be down temporarily.
2023	Confidentiality	Data breach	Airline	Sweden	Scandinavian airline SAS was hit by data breach attacks, and hackers paralyzed the carrier's website and leaked customer information from its app.
2023	Availability	Data breach	Hotel	U.S.	Choice Hotels International confirmed that guest data from its Radisson Hotels Americas chain was compromised as part of the massive MOVEit file transfer system hack carried out by the Cl0p ransom gang.
2023	Confidentiality	Ransomware	Restaurant	U.S.	Pizza Hut, KFC, and Taco Bell companies advised a number of individuals that their personal data were exposed during a ransomware attack
2023	Confidentiality	Data breach	Online payment system	U.S.	PayPal suffered a data breach attack in which the hackers were able to access PayPal customer accounts using stolen login credentials.
2023	Availability	Hacking	Hotel	U.S.	The Marriot Hotel group suffered a data breach attack after a hacking group tricked an employee and subsequently gained computer access.
2023	Availability	Ransomware	OTA	U.K.	Scenic Group was exposed to a ransomware attack in February 2023.

2023	Availability	SQL injection	Entertainment	Netherlands	Landal Greenparks reported a data breach attack. This cyberattack compromised personal information, including names, birth dates, genders, addresses, and email addresses.
2023	Confidentiality	DDoS	Hotel/OTA	Spain	DMO website of Spain (Spain.info), Paradores, Riu, Majestic, Petit Palace, Only You, Catalonia Hotels & Resorts websites, and OTAs' Reservalis and Best Hotels were attacked by a DDoS. This attack was made by the pro-Russian group called NoName057.

Nonetheless, the diversity of cyberattack methods shown in Table 1 reveals the importance of cybersecurity in the travel and tourism industries. For this reason, we were forced to stage the reality of cyberattack scenarios in both sectors that can be tackled in a cybersecurity culture framework by OTAs, hotels, and tour operators. These data are illustrated in Table 2, which displays a review of documented cyberattacks in the travel and tourism industries in the period established. The categorization of the number of cyberattacks is shown in Table 3. These findings will help smart cities, travel and tourism companies, and cybersecurity researchers to make better decisions in the future, and it is very important to document cases of cyberattacks at OTAs, travel, and the tourism literature.

Table 3. Total cyberattacks by category.

Category of Attack	Hotel	OTA	Airlines	Entertainment	Restaurant	Supermarket	Airport	Bus Transport	Marketing	Travel Reservation System	Online Payment System	Technology
Data breach	11	4	7				1	2		1	1	
Malware	7	1			1							
Ransomware	2	1		1	1	1						
Phishing	1	1										
Hacking	2	2	1	1								
DDoS	2	1					1					
Website/app breach						1			1			
POS					1							
Bot	1											
Human error						1						
SQL injection				1								
Zero-day exploit												1
Total	26	10	8	3	3	3	2	2	1	1	1	1

Our final sample includes 61 cyberattacks affecting OTA, hotel, restaurant, and airline firms such as Marriot Hotels, Wyndham Hotels, Hyatt Hotels, Intercontinental Hotel Group, Mandarin Oriental Hotel Group, Booking.com, FTI company, Sabre Corporation, Orbits and Expedia travel agencies, EasyJet and Air France airlines, Pizza Hut, KFC, Taco Bell, among many others. Most of the cyberattacks shown in Table 2 are linked with data breach/malware/ransomware identity theft, addresses, login credentials, bank account numbers, credit card numbers, and booking details. Each attack included in our sample occurred on a different date and/or involved different OTAs, hotels, and restaurants located in different geographical areas and cities [29]. Moreover, we are confident that the travel and tourism industries have suffered more than 61 cyberattacks, the issue is that not all companies report cyberattacks committed because these incidents affect the

reputation of companies and their corporate image, as well as consumer trust. Panai [104] notes that no one knows the full extent of cyberattacks being committed on the Internet.

4. Findings and Discussion

Cyberattack Incidents in the Travel and Hospitality Industries

Cybersecurity is a mandatory asset for smart cities, travel, and tourism companies because they struggle with the complexity of digital security and possible cyberattacks. For instance, hotels have intensified their online presence through web direct sales to reduce their dependence on OTA commissions [105], and this has provided a powerful incentive for attacks by hackers and cybercriminals. Table 2 presents a timeline of cyberattacks on the travel and tourism industries since 2000. This illustrates documented and classified cyberattacks around the world by year, the type of cyberattack, location, and the cyberattack description, with the aim of achieving the main objective of this manuscript, which is to analyse the cybersecurity in OTA and hotel sectors to protect consumer's private data in smart cities.

In the period analysed (2000–2023), 61 cyberattacks were documented and analysed. Hotels were the most affected by cyberattacks with 26 incidents, followed by OTAs with 10, airlines (8), entertainment (3), restaurants (3), supermarkets (3), airports (2), bus transport (2), travel reservation systems (1), online payments systems (1), marketing (1), and technology with 1 cyberattack incident. All these sectors are related to e-commerce activities, and they were necessary to include in this research, as we can see in Tables 2 and 3. Obviously, all these cyberattacks had negative impacts on smart cities and their brand image because some tourists had bad experiences during their holidays after the companies were hacked, which had immediate consequences such as customer credit and debit cards and tourists' personal information being exposed to hackers. Cybersecurity is a crucial aspect of smart city development, as it aims to protect the information and communication systems of citizens and companies [106]. We are completely sure that there have been over 61 cyberattacks in the tourism industry. Indeed, there were 775 cyberattacks on airlines and 150 at airports in 2020 [107], but most of these cyberattack incidents are not published for national security and social alarm reasons.

The findings of this study reveal that hotels and OTAs are constantly exposed to cyberattacks, especially by data breaches and malware attacks (Table 3), and the consequences of these incidents are severe for both guests and firms. Shabani and Munir [108] suggest that the techniques currently utilised by hotels and OTAs to prevent cyberattacks are mostly rudimentary and outdated [109]. Hotel and OTA sectors are among the most vulnerable to data breaches, due to the volume of personal and credit card information processed daily [110], without forgetting that most hotels use OTAs as one of their main distribution channels. In this study, we recommend OTA and hotel operators understand the nature and outcome of the incident to respond immediately to new threats, and to communicate this serious problem to all of those affected. OTA and hospitality companies must weigh the risks like a data breach against the costs associated with both compliance and noncompliance. For example, GDPR-imposed fines and fees can reach EUR 20 million [111].

Another aspect to be highlighted is that in the total cyberattacks that occurred in the period examined, hackers or cybercriminals illegally accessed payment transactions and users' credit card numbers in 22 cyberattacks, especially in data breach attacks. These data confirm the previous findings of Gwebu and Barrows [112] and Wang et al. [113], which revealed that data breaches are becoming more common and publicised in travel and hospitality sectors [114]. For instance, a data breach in a marketing company that manages the advertising, promotion, and marketing practices of McDonald's, Coca-Cola, Shell, Asus, hotels, and OTAs' websites had dire consequences not only for the firms involved but also for users' privacy. In many cases, the customers are not informed of these serious incidents. In 2013 and 2014, Yahoo and Equifax were hacked (data breach), and these two

firms did not report this incident until 2016 to the Securities and Exchange Commission (S.E.C) even though the information of millions of users was compromised [115].

Data breaches were the most frequent incidents in hotels with 11 attacks, followed by airlines with 7 attacks and OTAs with 4 attacks. AAG [103] reported that the rate and cost of data breaches are increasing in the travel and tourism sectors. Since 2001, the victim count has increased from 6 victims per hour to 97, representing a 1517% increase over 20 years. Regarding malware attacks, these have mainly concentrated on hotels such as White Lodging, Noble House, Starwood, Las Vegas, Hei, Millennium, and Omni hotels, all of which are localised in the U.S. The rest of the cyberattacks had a lesser impact on the sectors examined. In addition, the U.S. was the worst affected by cyberattacks with 34 incidents in the period established, followed by the U.K. with 6 incidents and the Netherlands with 3 incidents. These results are very similar to the AAG's report, which revealed that the U.S. was the most targeted country for cyberattacks, accounting for 46% of attacks globally, followed by the U.K. and the Netherlands [103]. Losing private information by companies is a direct loss of finances like lost fines, sales, or monetary judgments [116]. If a cyberattack involves insiders, companies are not interested in reporting it. On the contrary, if the objective is retrieving money or data back, then companies are very interested in informing law enforcement [117]. A recent study conducted by Dearden et al. [118] found that insiders cause more damage and cost more than outsider attacks; for this reason, one recommendation is to improve cybersecurity systems and strengthen the company's security culture.

That would mean that the situation would remain uncertain from the consumers' point of view. They only want a safe and personalised shopping experience when they buy a product or service through OTAs and hotels' websites and apps. Consumers need to feel secure and comfortable in the purchase processes, and companies need to preserve the security of the processing of their personal data and what they can do themselves to protect it against future cyberthreats and cyberattacks. The public policy and self-regulatory efforts to alleviate consumer privacy concerns by public and private organisations require greater control and protection over the management and dissemination of private data of users because, according to Phelps et al. [119], consumer concern and willingness to provide firms with personal data vary dramatically by information type. In light of existing and emerging privacy issues in travel and tourism companies, public and private organisations should seriously consider initiatives designed to guarantee and protect the purchasing processes and personal data of consumers against possible cyberattacks and the effects thereof.

The penalties imposed by governments are not sufficiently severe to restrain firms where there is no commitment to comply with consumer privacy concerns and experience through digital channels [120]. In the period analysed by this study, 95 per cent of cyberattacks affected the privacy of user data. This result is quite worrying as it shows how every day, companies are victims of cyberattacks that compromise the security of the privacy of user data. Flavián and Guinalíu [121] revealed that an individual's loyalty to a website is closely linked to the levels of trust and security perceived by consumers regarding the handling of their private data. New research studies are required to tackle tourists' privacy decision-making process in order to ensure they are making informed decisions when it comes to sharing personal information while travelling [122].

These results suggest that travel and tourism companies should first inform the police and government authorities, and second, report these cyberattacks to smart cities to prevent other possible cyberattacks or cyberthreats. Cybersecurity protocols need to be implemented by all travel and companies in smart cities to avoid new cyberthreats and cyberattacks; in fact, the current countermeasures are not effective in combating cyberattacks in the tourism industry according to our findings. Cybersecurity systems are essential in smart cities due to the increasing interconnectivity, widespread use of ICT, collection of users' data, monitoring of critical infrastructures, optimization of tourism services, and tourists' experiences at tourist attractions. Hence, cybersecurity prevention must be

an integral part of smart cities and companies' operating systems, because mitigating cyberthreats and cyberattacks requires better measurement, diversity of systems, interoperability, contingency plans, and the deliberate choice to avoid ubiquitous interconnection in critical systems. In short, this study suggests that an organisational cybersecurity culture should be included in smart cities and travel and tourism firms, as well as improving security protocols and systems to identify and prevent cyberattacks successfully. Combining cybersecurity and tourism activities in the development of smart cities is of paramount importance considering that smart city challenges are complex and multifaceted [123].

5. Conclusions

The findings of the current research prove that hotels and OTAs were constantly exposed to cyberattacks in the period analysed, especially by data breaches and malware attacks; in fact, this is the main novelty of this research. In addition, these incidents were severe for both guests and tourism companies because these vulnerabilities and their consequences affected the reputation of companies and their corporate image, as well as consumer confidence. According to our results, we suggest that travel and tourism companies should monitor and report the risks associated with users' private data based on the level of data exposure to protect and prevent possible vulnerabilities and avoid future cyberattacks. The results also showed that most cyberattacks examined in this manuscript were aimed at stealing the information of companies and users' private data such as email addresses, credit card numbers, security codes, and encoded magstripe data, among many others. Cyberattacks and cyberthreats never disappear completely in the travel and tourism sectors because these illegal activities are closely related to hacker's thirst for power, fame, and wealth. Moreover, we suggest that travel and tourism companies report cyberattack and cyberthreat incidents to the police, government authorities, and smart cities to prevent further harm to other firms and users.

The descriptive analysis of the types of cyberattacks (see Table 2) shows how the U.S. was the worst affected by cyberattacks, followed by the U.K. and the Netherlands. During the period examined in this research, 95% of cyberattacks affected the privacy of user data. Thus, the findings suggest that cyberattacks have negative impacts on OTA and tourism firms' websites and apps, which damage their reputation and brand image worldwide. So, data confidentiality, integrity, and availability are the key elements of cybersecurity that must be provided properly to avoid cyberattacks by companies and their workers. The manipulation of users' privacy and information deteriorates the sales performance of OTAs and hotels because of damaged customer trust and satisfaction. Most OTAs and hotels do not have crisis planning or management schemes to tackle crisis or cyberattack situations, or even contingency plans. For this reason, it is essential for hotel and OTA operators to prevent customer dissatisfaction due to the loss of their information and confidentiality by hackers and cybercriminals. Therefore, the responsibility of OTAs and hotels should focus on loyal clients while securing their private information and experience as an added value.

Finally, it must be noted that it is very common that customers are not immediately informed by companies when they suffer cyberattacks, as we mentioned previously, and the worst situation is that the information related to the incident is always late or simply never arrives. If firms aim to gain consumer confidence, then they also have to be sure that they protect their privacy. Both actions go hand-in-hand. Travel and tourism companies must be transparent in how they use consumers' personal information and how they communicate the potential benefits and risks of sharing their data. In this context, smart city managers, researchers, and travel and tourism operators must become clear that when a cyberattack hits a company or city, its negative consequences involve all public and private organisations, as well as residents and tourists. We should not forget that a smart city is a system of systems, where these are linked together to manage city services, and this digital synergy must ensure users' transactions and commercial activities in the entire city.

5.1. Contribution to Literature

From a theoretical perspective, this manuscript contributes to the cybersecurity literature by including different types of cyberattacks in the travel and tourism industries, as well as documenting new cases of cyberattacks in the tourism literature. Moreover, travel and tourism operators should improve the security and privacy features of their systems, together with emphasizing the safety features offered by their websites and apps [124]. However, firms have incentives to improve clients' private information sharing [125]. Smart cities, OTA operators, and hotel operators need to create a secure cyberspace culture for their employees, partners, suppliers, and customers to prevent future cyberattacks [3]. Our findings suggest that companies have great vulnerabilities in preventing cyberattacks and ensuring users' private data. Indeed, there is a lack of the right policy for cybercrime, and this is becoming a major problem in the travel and tourism industry. In the case of consumers, they should be aware of e-commerce fraud crime and the types of cyberattacks. Applying fraud detection web and app services in management by OTAs and hotels can greatly reduce the problem of vulnerabilities and cybercrimes [126,127]. Moreover, this manuscript also provides evidence that this topic requires greater efforts in terms of research, laws, and efficient safety tools to combat cyberattacks in the travel and tourism industries by researchers, governments, and experts in cybersecurity.

5.2. Practical Implications

This paper also offers some practical implications. First, travel and tourism companies and smart cities should emphasise the relevance of proactive communication related to cyberattacks to enhance their cybersecurity protocols and strengthen customer relationships. Second, when the DMO website of Spain (Spain.info https://www.spain.info/es/ accessed on 1 February 2024), Paradores, Riu, Majestic, Petit Palace, Catalonia Hotels & Resorts websites, OTAs' Reservalis, and Best Hotels were hacked by the pro-Russian group called NoName057, this seriously affected the entire tourism industry and Spanish smart cities like Barcelona, Málaga, Benidorm, Gijón, Santander, Seville, among many others. This study also adds relevant information related to the impact of OTA and hotel cyberattacks on smart cities and how regional and national governments should be aware that the cyberattacks of travel and tourism companies have negative effects on smart cities.

Therefore, it is clear that more effective national action is required in terms of interoperability, cybersecurity, and contingency plans against future cyberthreats and cyberattacks. In a nutshell, a cybersecurity culture in private and public organisations, and with cybersecurity cross-systems helps travel and tourism operators make better decisions against cyberattacks. Third, we recommend developing cybersecurity awareness campaigns by government bodies and companies to equip citizens and tourists with the necessary knowledge and skills to identify, prevent, and respond to cyberthreats. The benefit of this research for the field of security is that we provide a new point of view on cybersecurity in a tourism context, which shows that security in the tourism industry requires the hiring of cybersecurity experts to reduce cyberattacks in this sector.

5.3. Study Limitations and Future Research

There are several limitations in this research. First, this study was restricted to collecting cyberattacks in the travel and tourism sectors. Future studies can extend this scope to include other sectors in order to compare the levels of cybersecurity of companies and sectors or even to analyse consumers' perceptions of a cyberattack and their private data terms. Second, private and public organisations often do not admit to having suffered cyberattacks and cyberthreats for fear of negative publicity [36,128]. Therefore, future studies would be necessary to examine why companies are reluctant to provide information about cyberattacks suffered by hackers and cybercriminals to users and governments. Finally, this research did not include or document the efficacy of the cybersecurity

by companies against cyberattacks and cyberthreats, and this relevant information and data should be implemented in future research.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The author would like to thank anonymous reviewers and editors for providing valuable suggestions and comments.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Buhalis, D.; Leung, D.; Lin, M. Metaverse as a disruptive technology revolutionising tourism management and marketing. *Tour. Manag.* **2023**, *97*, 104724.
2. Magliulo, A. Cybersecurity and tourism competitiveness. *Eur. J. Tour. Hosp. Recreat.* **2016**, *7*, 128–134.
3. Paraskevas, A. Cybersecurity in travel and tourism: A risk-based approach. In *Handbook of e-Tourism*; Springer International Publishing: Cham, Swizerland, 2022; pp. 1605–1628.
4. Levy, Y.; Gafni, R. Introducing the concept of cybersecurity footprint. *Inf. Comput. Secur.* **2021**, *29*, 724–736.
5. Florido-Benítez, L. International mobile marketing: A satisfactory concept for companies and users in times of pandemic. *Benchmarking Int. J.* **2022**, *29*, 1826–1856.
6. Bai, H.; Ran, W. Analysis of the Vulnerability and Resilience of the Tourism Supply Chain under the Uncertain Environment of COVID-19: Case Study Based on Lijiang. *Sustainability* **2020**, *14*, 2571.
7. Talwar, S.; Dhir, A.; Kaur, P.; Mäntymäki, M. Barriers toward purchasing from online travel agencies. *Int. J. Hosp. Manag.* **2020**, *89*, 102593.
8. Luo, S.; Choi, T.M. E-commerce supply chains with considerations of cyber-security: Should governments play a role? *Prod. Oper. Manag.* **2022**, *31*, 2107–2126.
9. Verhulsdonck, G.; Weible, J.L.; Helser, S.; Hadjuck, N. Smart Cities, Playable Cities, and Cybersecurity: A Systematic Review, International Journal of Human–Computer Interaction. *Int. J. Hum.–Comput. Interact.* **2023**, *39*, 378–390.
10. Florido-Benítez, L. Identifying cybersecurity risks in Spanish airports. *Cyber Secur.* **2021**, *4*, 267–291.
11. Vitunskaite, M.; He, Y.; Brandstetter, T.; Janicke, H. Smart cities and cybersecurity: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Comput. Secur.* **2019**, *83*, 313–331.
12. Alasali, F.; Itradat, A.; Abu Ghalyon, S.; Abudayyeh, M.; El-Naily, N.; Hayajneh, A.M.; AlMajali, A. Smart Grid Resilience for Grid-Connected PV and Protection Systems under Cyber Threats. *Smart Cities* **2024**, *7*, 51–77.
13. Tutak, M.; Brodny, J. A Smart City Is a Safe City: Analysis and Evaluation of the State of Crime and Safety in Polish Cities. *Smart Cities* **2023**, *6*, 3359–3392.
14. Morrison, A.M.; Buhalis, D. *Routledge Handbook of Trends and Issues in Tourism Sustainability, Planning and Development, Management, and Technology*; Routledge: London, UK, 2024.
15. D'Adamo, I.; González-Sánchez, R.; Medina-Salgado, M.S.; Settembre-Blundo, D. E-Commerce Calls for Cyber-Security and Sustainability: How European Citizens Look for a Trusted Online Environment. *Sustainability* **2021**, *13*, 6752.
16. Chan, H.K.; He, H.; Wang, W.Y. Green marketing, and its impact on supply chain management in industrial markets. *Ind. Mark. Manag.* **2012**, *41*, 557–562.
17. Chen, H.S.; Fiscus, J. The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *J. Hosp. Tour. Technol.* **2018**, *9*, 223–234.
18. PhocusWire. The New Ways Cybercriminals Are Attacking Travel Companies. 2022. Available online: https://www.phocuswire.com/cybercriminals-find-new-ways-to-attack-travel-companies (accessed on 22 February 2023).
19. Berezina, K.; Cobanoglu, C.; Miller, B.L.; Kwansa, F.A. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *Int. J. Contemp. Hosp. Manag.* **2012**, *24*, 991–1010.
20. Pizam, A.; Ozturk, A.B.; Hacikara, A.; Zhang, T.; Balderas-Cejudo, A.; Buhalis, D.; Fuchs, G.; Hara, T.; Meira, J.; Revilla, R.G.M.; et al. The role of perceived risk and information security on customers' acceptance of service robots in the hotel industry. *Int. J. Hosp. Manag.* **2024**, *117*, 103641.
21. Alawida, M.; Omolara, A.E.; Abiodun, O.I.; Al-Rajab, M. A deeper look into cybersecurity issues in the wake of COVID-19: A survey. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 8176–8206.
22. Khursheed, A.; Kumar, M.; Sharma, M. Security against cyberattacks in food industry. *Int. J. Control Theory Appl.* **2016**, *9*, 8623–8628.
23. Tong, L.; Kong, A.; Kwan, M. How to design and strengthen cyber security to cope with data breach in the hotel industry? In Proceedings of the Main Conference Proceedings 2022, Virtual, 22–25 May 2022; p. 61.
24. Fragniere, E.; Yagci, K. Network & cyber security in hospitality and tourism. In *Hospitality & Tourism Information Technology*; Cobanoglu, C., Dogan, S., Berezina, K., Collins, G., Eds.; USF M3 Publishing: Orlando, FL, USA, 2021; pp. 1–21.
25. Singh, P.; Rajput, R.S. Cybersecurity analysis in the context of digital wallets. *Int. J. Adv. Stud. Sci. Res.* **2019**, *4*, 522–525.
26. Lee, I. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet* **2020**, *12*, 157.

27. Bimaruci, H.; Hudaya, A.; Ali, H. Model of consumer trust on travel agent online: Analysis of perceived usefulness and security on re-purchase interests (case study ticket. com). *Dinasti Int. J. Econ. Financ. Account.* **2020**, *1*, 110–124.
28. Liu, X.; Ahmad, S.F.; Anser, M.K.; Ke, J.; Irshad, M.; Ul-Haq, J.; Abbas, S. Cybersecurity threats: A never-ending challenge for e-commerce. *Front. Psychol.* **2022**, *13*, 927398.
29. Arcuri, M.C.; Gai, L.; Ielasi, F.; Ventisette, E. Cyberattacks on hospitality sector: Stock market reaction. *J. Hosp. Tour. Technol.* **2020**, *11*, 277–290.
30. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain. Cities Soc.* **2019**, *50*, 101660.
31. Iranmanesh, M.; Ghobakhloo, M.; Nilashi, M.; Tseng, M.L.; Yadegaridehkordi, E.; Leung, N. Applications of disruptive digital technologies in hotel industry: A systematic review. *Int. J. Hosp. Manag.* **2022**, *107*, 103304.
32. Chin, K. Cybersecurity in the Hospitality Industry: Challenges and Solutions. 2023. Available online: https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry (accessed on 29 January 2024).
33. Bhattacharya, S.; Sharma, R.P.; Gupta, A. Does e-retailer's country of origin influence consumer privacy, trust and purchase intention? *J. Consum. Mark.* **2023**, *40*, 248–259.
34. Aftergood, S. Cybersecurity: The cold war online. *Nature* **2017**, *547*, 30–31.
35. Sarker, I.H.; Kayes, A.S.M.; Badsha, S.; Algahtani, H.; Watters, P.; Ng, A. Cybersecurity data science: An overview from machine learning perspective. *J. Big Data* **2020**, *7*, 41.
36. Boto-García, D. Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. *J. Hosp. Tour. Manag.* **2023**, *55*, 240–247.
37. Demertzi, V.; Demertzis, S.; Demertzis, K. An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. *Appl. Sci.* **2023**, *13*, 790.
38. De Arroyabe, I.F.; Arranz, C.F.; Arroyabe, M.F.; de Arroyabe, J.C F. Cybersecurity capabilities and cyberattacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. *Comput. Secur.* **2023**, *124*, 102954.
39. Corallo, A.; Lazoi, M.; Lezzi, M.; Luperto, A. Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Comput. Ind.* **2022**, *137*, 103614.
40. UNWTO. Supporting Jobs and Economies through Travel & Tourism. Call for Action to Mitigate the Socio-Economic Impact of COVID-19 and Accelerate Recovery. 2020. Available online: https://webunwto.s3.eu-west-1.amazonaws.com/s3fs-public/2020-04/COVID19_Recommendations_English_1.pdf (accessed on 10 July 2023).
41. Yallop, A.C.; Gică, O.A.; Moisescu, O.I.; Coroș, M.M.; Séraphin, H. The digital traveller: Implications for data ethics and data governance in tourism and hospitality. *J. Consum. Mark.* **2023**, *40*, 155–170.
42. European Union. What Is GDPR, the EU's New Data Protection Law? 2023. Available online: https://gdpr.eu/what-is-gdpr/ (accessed on 13 March 2023).
43. Hellard, B. Tourism Platforms Sign Data-Sharing Deal with EU. 2020. Available online: https://www.itpro.com/policy-legislation/data-governance/354933/tourism-platforms-sign-data-sharing-deal-with-eu (accessed on 27 May 2023).
44. Fernandes, T.; Costa, M. Privacy concerns with COVID-19 tracking apps: A privacy calculus approach. *J. Consum. Mark.* **2023**, *40*, 181–192.
45. Hauff, C.J.; Nilsson, J. Individual costs and societal benefits: The privacy calculus of contact-tracing apps. *J. Consum. Mark.* **2023**, *40*, 171–180.
46. Alsmadi, I. Software Management. In *The NICE Cyber Security Framework*; Springer: Cham, Swizerland, 2020.
47. Cooper, D.A.; Yalcin, T.; Nistor, C.; Macrini, M.; Pehlivan, E. Privacy considerations for online advertising: A stakeholder's perspective to programmatic advertising. *J. Consum. Mark.* **2023**, *40*, 235–247.
48. Malgieri, G. In/acceptable marketing and consumers' privacy expectations: Four tests from EU data protection law. *J. Consum. Mark.* **2023**, *40*, 209–223.
49. Elgarhy, S.D. Effects of service quality, loyalty programs, pricing strategies, and customer engagement on firms' performance in Egyptian travel agencies: Mediating effects of customer retention. *J. Qual. Assur. Hosp. Tour.* **2022**, *24*, 753–781.
50. Buhalis, D. Strategic use of information technologies in the tourism industry. *Tour. Manag.* **1998**, *15*, 409–421.
51. Florido-Benítez, L. The impact of tourism promotion in tourist destinations: A bibliometric study. *Int. J. Tour. Cities* **2022**, *8*, 844–882.
52. GlobalData. Cybersecurity in Travel and Tourism—Thematic Intelligence. 2023. Available online: https://www.globaldata.com/store/report/cybersecurity-in-travel-tourism-theme-analysis/ (accessed on 15 June 2023).
53. Shengenvisa. Cyberattacks Increased by 60% in Tourism Sector This Year. 2022. Available online: https://www.schengenvisainfo.com/news/cyberattacks-increased-by-60-in-tourism-sector-this-year/ (accessed on 3 January 2024).
54. Airport Technology. Cybersecurity: A Key Theme in the Travel Industry. 2023. Available online: https://www.airport-technology.com/features/cybersecurity-a-key-theme-in-the-travel-industry/ (accessed on 23 February 2023).
55. Post. A. The Cybersecurity Risks of Smart City Technologies: What Do the Experts Think? 2023. Available online: https://cltc.berkeley.edu/publication/smart-cities/ (accessed on 2 January 2024).
56. Ordóñez-Martínez, D.; Seguí-Pons, J.M.; Ruiz-Pérez, M. Conceptual Framework and Prospective Analysis of EU Tourism Data Spaces. *Sustainability* **2024**, *16*, 371.

57. Medium.com. The History Of Hotels Cyber Attacks. 2020. Available online: https://securestay.medium.com/the-history-of-hotels-cyber-attacks-4b6a09c8bf30 (accessed on 17 December 2023).
58. Scott, N.; Laws, E.; Prideaux, B. *Safety and Security in Tourism: Recovery Marketing After Crises*; Routledge: Abingdon, UK, 2010.
59. Prabhu, B.A.; Dani, R.; Bhatt, C. A study of the challenges faced by the hotel sector with regards to cybersecurity. In *Automation and Computation*; CRC Press: Boca Raton, FL, USA, 2023; pp. 284–294.
60. Al-Dosari, K.; Fetais, N.; Kucukvar, M. A shift to green cybersecurity sustainability development: Using triple bottom-line sustainability assessment in Qatar transportation sector. *Int. J. Sustain. Transp.* **2023**, *17*, 1287–1301.
61. Mungo, J. Self-paced cybersecurity awareness training educating retail employees to identify phishing attacks. *J. Cyber Secur. Technol.* 2023, *in press*. https://doi.org/10.1080/23742917.2023.2244210.
62. Wynn, M.; Lam, C. Digitalisation and IT Strategy in the Hospitality Industry. *Systems* **2023**, *11*, 501.
63. Durst, S.; Hinteregger, C.; Zieba, M. The effect of environmental turbulence on cyber security risk management and organizational resilience. *Comput. Secur.* **2024**, *137*, 103591.
64. Dodge, M.; Kitchin, R. The challenges of cybersecurity for smart cities. In *Creating Smart Cities*; Routledge: London, UK, 2018, 205–216.
65. Sheridan, K. Destructive Malware Attacks up 200% in 2019. 2019. Available online: https://www.darkreading.com/endpoint/destructive-malware-attacks-up-200-in-2019 (accessed on 6 January 2024).
66. Chaganti, R.; Bhushan, B.; Ravi, V. A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges, and future directions. *Comput. Commun.* **2022**, *197*, 96–112.
67. Elliot, C. Hackers Are Targeting Airlines in Record Numbers. Here's What That Means for You. 2019. Available online: https://www.forbes.com/sites/christopherelliott/2019/02/25/hackers-are-targeting-airlines-in-record-numbers-heres-what-that-means-for-you/ (accessed on 1 February 2023).
68. Schlackl, F.; Link, N.; Hoehle, H. Antecedents and consequences of data breaches: A systematic review. *Inf. Manag.* **2022**, *59*, 103638.
69. Al-Shareeda, M.A.; Anbar, M.; Manickam, S.; Hasbullah, I.H. Password-guessing attack-aware authentication scheme based on Chinese remainder theorem for 5G-enabled vehicular networks. *Appl. Sci.* **2022**, *12*, 1383.
70. Muñoz, A.; Fernández-Gago, C.; López-Villa, R. A test environment for wireless hacking in domestic IoT scenarios. In *Mobile Networks and Applications*; Springer: Berlin/Heidelberg, Germany, 2022.
71. Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. CyberSecurity Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146.
72. Smith, A.D.; Rupp, W.T. Issues in cybersecurity; understanding the potential risks associated with hackers/crackers. *Inf. Manag. Comput. Secur.* **2002**, *10*, 178–183.
73. Huang, J.; Ho, D.W.; Li, F.; Yang, W.; Tang, Y. Secure remote state estimation against linear man-in-the-middle attacks using watermarking. *Automatica* **2020**, *121*, 109182.
74. Le Coze, J.C. The 'new view' of human error. Origins, ambiguities, successes, and critiques. *Saf. Sci.* **2022**, *154*, 105853.
75. Deshpande, A.; Patil, I.; Bhave, J.; Giri, A.; Sable, N.P.; Chavan, G.T. Detection and Notification of Zero-Day attack to Prevent Cybercrime. In Proceedings of the 2023 4th International Conference for Emerging Technology (INCET), Belgaum, India, 26–28 May 2023; IEEE: Piscataway, NJ, USA, 2023; pp. 1–5.
76. Olding, A.; Turner, P. Cyber vulnerabilities and the tourism industry: Developing a conceptual framework. In Proceedings of the ACIS 2007 Proceedings, Toowoomba, Australia, 5–7 December 2007; pp. 848–855.
77. Chin, K. Biggest Data Breaches in US History. 2023. Available online: https://www.upguard.com/blog/biggest-data-breaches-us (accessed on 19 July 2023).
78. ISACA. The Impact of Cybersecurity on Consumer Behaviour. 2022. Available online: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/the-impact-of-cybersecurity-on-consumer-behavior (accessed on 31 December 2023).
79. Bonastre, L.; Granollers, T. A set of heuristics for user experience evaluation in e-commerce websites. In Proceedings of the 7th International Conference on Advances in Computer-Human Interactions IARIA, Barcelona, Spain, 23–27 March 2014; pp. 27–34.
80. *ISO 9241-210:2010*; Ergonomics of Human-System Interaction—Part 210: Human-Centred Design for Interactive Systems. ISO: Geneva, Switzerland, 2010. Available online: https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en (accessed on 3 August 2023).
81. Ritter, M.; Winterbottom, C. *UX for the Web: Build Websites for User Experience and Usability*; Packt Publishing Ltd.: Birmingham, UK, 2017.
82. Anichiti, A.; Dragolea, L.L.; Tacu-Hârșan, G.D.; Haller, A.P.; Butnaru, G.I. Aspects Regarding Safety and Security in Hotels: Romanian Experience. *Information* **2021**, *12*, 44.
83. Eurocontrol. Aviation Under Attack from a Wave of Cybercrime. 2021. Available online: https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime (accessed on 1 May 2023).
84. Ye, B.H.; Fu, H.; Law, R. Use of impact-range performance and asymmetry analyses to improve OTA website quality. *J. Hosp. Tour. Manag.* **2016**, *26*, 9–17.
85. Tsang, N.K.; Wong, O. Traveller's adoption of travel advisory system: A case of Hong Kong's outbound travel alert system. *J. Travel Tour. Mark.* **2021**, *38*, 213–231.

86. Chen, J.S.; Kamalanon, P.; Janupiboon, T.P. Company websites and mobile apps versus social media: Which service experience creates more customer value for online travel agencies? *Serv. Bus.* **2022**, *16*, 1081–1110.
87. Chan, I.C.C.; Ma, J.; Law, R.; Buhalis, D.; Hatter, R. Dynamics of hotel website browsing activity: The power of informatics and data analytics. *Ind. Manag. Data Syst.* **2021**, *121*, 1398–1416.
88. Park, Y.A.; Gretzel, U.; Sirakaya-Turk, E. Measuring web site quality for online travel agencies. *J. Travel Tour. Mark.* **2007**, *23*, 15–30.
89. Dong-Her, S.; Hsiu-Sen, C.; Chun-Yuan, C.; Lin, B. Internet security: Malicious e-mails detection and protection. *Ind. Manag. Data Syst.* **2004**, *104*, 613–623.
90. Cao, K.; Yang, Z. A study of e-commerce adoption by tourism websites in China. *J. Destin. Mark. Manag.* **2016**, *5*, 283–289.
91. Ali, S.A.; Elsaid, S.A.; Ateya, A.A.; ElAffendi, M.; El-Latif, A.A.A. Enabling Technologies for Next-Generation Smart Cities: A Comprehensive Review and Research Directions. *Future Internet* **2023**, *15*, 398.
92. United Nations. *World Population Prospects: 2017 Revision*; Department of Economic and Social Affairs: New York, NY, USA, 2022. Available online: https://population.un.org/wpp/ (accessed on 1 January 2024).
93. BT Group. Cybercrime: More Than 500 Potential Attacks Clocked Every Second. 2023. Available online: https://newsroom.bt.com/cybercrime-more-than-500-potential-attacks-clocked-every-second/ (accessed on 3 January 2024).
94. Barcik, P.; Coufalikova, A.; Frantis, P.; Vavra, J. The Future Possibilities and Security Challenges of City Digitalization. *Smart Cities* **2023**, *6*, 137–155.
95. Fabrègue, B.F.G.; Bogoni, A. Privacy and Security Concerns in the Smart City. *Smart Cities* **2023**, *6*, 586–613.
96. Florido-Benítez, L. Constructing Spanish smart destinations: A new guide for the tourism industry. *Int. J. Tour. Cities* 2024, *in press*. https://doi.org/10.1108/IJTC-09-2023-0193.
97. Coca-Stefaniak, A.; Morrison, A.M. City tourism destinations and terrorism a worrying trend for now, but could it get worse? *Int. J. Tour. Cities* **2018**, *4*, 409–412.
98. Jones, R. EasyJet Hacking Attack: Are You Affected and What Should You Do? 2020. Available online: https://www.theguardian.com/business/2020/may/19/easyjet-hacking-attack-what-to-do-customers (accessed on 5 January 2024).
99. Javed, A.R.; Shahzad, F.; ur Rehman, S.; Zikria, Y.B.; Razzak, I.; Jalil, Z.; Xu, G. Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects. *Cities* **2022**, *129*, 103794.
100. Bekkali, A.E.; Essaaidi, M.; Boulmalf, M. A Blockchain-Based Architecture and Framework for Cybersecure Smart Cities. *IEEE Access* **2023**, 11, 76359–76370.
101. CSIS. Significant Cyber Incidents Since 2006. 2023. Available online: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (accessed on 24 July 2023).
102. KonBriefing. Cyberattacks on the Aviation Industry in 2022. 2023. Available online: https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html#Res478761 (accessed on 1 August 2023).
103. AAG. The Latest 2023 Cyber Crime Statistics. 2023. Available online: https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Cyber%20crime%20in%20the%20United,for%2046%25%20of%20attacks%20globally (accessed on 3 August 2023).
104. Panai, E. A Cybersecurity framework for independent hotels. In Proceedings of the 4th EATSA-FRANCE 2018, Challenges of Tourism Development, Dijon, France, 18–22 June 2018; pp. 145–152.
105. Yin, H.C.; Goh, E.; Law, R. Developing inter-organizational relationships with online travel agencies (OTAs) and the hotel industry. *J. Travel Tour. Mark.* **2019**, *36*, 428–442.
106. Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities* **2023**, *6*, 1523–1544.
107. Alohali, B.A. Aviation Cybersecurity National Governance. 2023. Available online: https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/2.2%20Saudi%20Arabia%20-%20Aviation%20Cybersecurity%20National%20Governance.pdf (accessed on 29 January 2024).
108. Shabani, N.; Munir, A. A Review of Cyber Security Issues in Hospitality Industry. In *Intelligent Computing. SAI 2020. Advances in Intelligent Systems and Computing*; Arai, K., Kapoor, S., Bhatia, R., Eds.; Springer: Cham, Swizerland, 2020; Volume 1230, pp. 82–493.
109. Wicaksono, A.; Maharani, A. The effect of perceived usefulness and perceived ease of use on the technology acceptance model to use online travel agency. *J. Bus. Manag. Rev.* **2020**, *1*, 313–328.
110. Thomaidis, A. *Data Breaches in Hotel Sector According to General Data Protection Regulation (EU 2016/679)*; Valeri, M., Ed.; Tourism Risk, Emerald Publishing Limited: Bingley, UK, 2022; pp. 129–140.
111. GDPR. What are the GDPR Fines? 2023. Available online: https://gdpr.eu/fines/ (accessed on 7 June 2023).
112. Gwebu, K.; Barrows, C.W. Data breaches in hospitality: Is the industry different? *J. Hosp. Tour. Technol.* **2020**, *11*, 511–527.
113. Wang, X.; Wang, X.; Liu, Z.; Chang, W.; Hou, Y.; Zhao, Z. Too generous to be fair? Experiments on the interplay of what, when, and how in data breach recovery of the hotel industry. *Tour. Manag.* **2022**, *88*, 104420.
114. Gitlin, M.; Goldstein, M.J. *Cyberattack*; Twenty-First Century Books: Minneapolis, MN, USA, 2015.
115. Newman, C.A. When to Report a Cyberattack? For Companies, That's Still a Dilemma. 2018. Available online: https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html (accessed on 25 December 2023).

116. Sahu, A.K.; Gutub, A. Improving grayscale steganography to protect personal information disclosure within hotel services. *Multimed. Tools Appl.* **2022**, *81*, 30663–30683.
117. Swinhoe, D. Why Businesses Don't Report Cybercrimes to Law Enforcement. 2019. Available online: https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html (accessed on 6 January 2024).
118. Dearden, T.E.; Parti, K.; Hawdon, J.; Gainey, R.; Vandecar-Burdin, T.; Albanese, J. Differentiating Insider and Outsider Cyberattacks on Businesses. *Am. J. Crim. Justice* **2023**, *48*, 871–886.
119. Phelps, J.; Nowak, G.; Ferrell, E. Privacy Concerns and Consumer Willingness to Provide Personal Information. *J. Public Policy Mark.* **2000**, *19*, 27–41.
120. Culnan, M.J.; Bies, R.J. Consumer Privacy: Balancing Economic and Justice Considerations. *J. Soc. Issues* **2003**, *59*, 323–342.
121. Flavián, C.; Guinalíu, M. Consumer trust, perceived security, and privacy policy: Three basic elements of loyalty to a web site. *Ind. Manag. Data Syst.* **2006**, *106*, 601–620.
122. Tussyadiah, I.; Li, S.; Miller, G. Privacy Protection in Tourism: Where We Are and Where We Should Be Heading For. In *Information and Communication Technologies in Tourism 2019*; Pesonen, J., Neidhardt, J., Eds.; Springer: Cham, Swizerland, 2019.
123. Almeida, F. Prospects of Cybersecurity in Smart Cities. *Future Internet* **2023**, *15*, 285.
124. Chong, A.Y.L.; Blut, M.; Zheng, S. Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia. *Decis. Support Syst.* **2022**, *53*, 34–43.
125. Cai, Z.; Liu, H.; Huang, Q.; Kang, Y.; Liang, L. Encouraging client's knowledge sharing in enterprise system post-implementation through psychological contract and entrepreneurial orientation. *Inf. Technol. People* **2020**, *33*, 689–709.
126. Saputra, R.W. A survey of cybercrime in Indonesia. In Proceedings of the 2016 International Conference on ICT For Smart Society (ICISS), Surabaya, Indonesia, 20–21 July 2016; IEEE: Piscataway, NJ, USA, 2016; pp. 1–5.
127. Babu, K.E.K. The Reality of Cybersecurity in Bangladesh, Relevant Laws, Drawbacks and Challenges. In *Cybersecurity in the Age of Smart Societies*; Advanced Sciences and Technologies for Security Applications; Jahankhani, H., Ed.; Springer: Cham, Swizerland, 2023.
128. Hall, C.M. Travel Safety, Terrorism, and the Media: The Significance of the Issue-Attention Cycle. *Curr. Issues Tour.* **2022**, *5*, 458–466.