Cybersecurity in travel and tourism: a risk-based approach

Paraskevas, Alexandros ORCID: https://orcid.org/0000-0003-1556-5293 (2020) Cybersecurity in travel and tourism: a risk-based approach. In: Handbook of e-Tourism. Springer Nature, Cham, Switzerland. ISBN 978303005324 6 (In Press)

http://dx.doi.org/10.1007/978-3-030-05324-6

This is the Accepted Version of the final output.

UWL repository link: https://repository.uwl.ac.uk/id/eprint/6761/

Cybersecurity in Travel and Tourism: A Risk-based Approach

Prof. Alexandros Paraskevas (PhD)
University of West London

Abstract

As the travel and tourism sector is embracing emerging technologies to redefine products, services, and consumer experiences, their cyber ecosystems become increasingly vulnerable to security risks related with these technologies, the huge amount of financial transactions they carry out and the valuable customer data they store. Over the last few years, several high-profile organizations in the sector made negative headlines because they did not pay appropriate attention to these risks and took an approach to cybersecurity that was fragmented, technology-focused and compliance-oriented. It is evident that a step change is needed, and this chapter presents a more comprehensive, business-driven and risk-based approach to building cybersecurity capability in an organization. The chapter starts with the business case for a cybersecurity strategy and then unfolds the components of a risk-based approach to cybersecurity.

Keywords: cyberattacks**;** cybersecurity; data breach; risk-based approach; threat actors; travel networks

1. Introduction

With the 'stone years' of simple internet adoption in their business models long past, many organizations in the travel and tourism sector are now navigating the so-called Fourth Industrial Revolution (also known as Industry 4.0) and embrace emerging technologies to redefine products, services, and consumer experiences (Schwab 2017). Change and digitization (i.e., the conversion of analogue to digital) are driven in ways that are exciting and often challenging to keep pace with, disrupting businesses, creating new markets and turning the world increasingly connected with continuous innovation. As the world is becoming smaller, cyber is getting bigger and moving into many new directions helping to fuel an unprecedented rise in consumer and business partners' expectations. It is expanding beyond the organization's four walls and IT environments and moves into the products and services they offer as well as into the partner, supplier, customer and stakeholder networks they create. However, this digital transformation in travel and tourism which involves online transactions, customer analytics, cloud integration, connected devices, and digital payment technology also leads to the realisation that, by growing their digital footprint, organizations are increasingly exposed to cyber threats.

Cyberattacks can be significantly detrimental to customer trust and brand reputation and often have severe financial, legal and regulatory implications. Kaspersky Lab (2018) estimates that it costs more than $500,000 to recover from a security breach. These are only direct losses: money businesses are forced to spend on IT recovery services, to cover lost business and downtime as well as legal and public relations services. Indirect losses i.e., costs for additional staff hiring and training, infrastructure upgrades etc. are estimated, on average, $70,000. Then there are fines to be paid. Three data breaches in Wyndham Hotels and Resorts' computer network between 2008 and 2010 compromised records of over 600,000 guests with $10.6 million of fraudulent credit card charges resulting not only at a lawsuit from the US Federal Trade Commission in 2012 but also from a shareholder in 2014. The shareholder filed a lawsuit against the company and its board directors and officers, claiming that their failure to implement adequate cybersecurity measures and disclose the data breaches in a timely manner caused shareholders to suffer the damages of an FTC investigation (Robinson 2014). Both lawsuits were settled for undisclosed amounts. Marriott International received in 2019 a fine of $124 million from the UK Information Commissioner's Office under the General Data Protection Regulation (GDPR), for one of the biggest data breaches in history where personal information of 500 million guests was exposed by a hack in the reservation database for its Starwood properties. The same regulator proposed a record $230 million fine against British Airways for failing to protect passenger data in a 2018 data breach (Olson 2019).

In response to this new threat environment, organizations spend huge amounts of money on cybersecurity. In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 it was expected to be worth more than $120 billion (a growth of roughly 35 times over 13 years). According to Gartner Inc (2018), worldwide spending on information security alone (a subset of the broader cybersecurity market) products and services exceeded $114 billion in 2018, an increase of 12.4%

from 2017. For 2019, they forecast the market to grow to $124 billion, and $170.4 billion in 2022. Yet, there has been a real lack of meaningful and sustainable success in preventing cyberattacks with cybercriminals upping their game and escalating their attacks with increased levels of sophistication whilst causing significant damage to many organizations. The May 2017 WannaCry cyberattack, for example, which allegedly involved the cybercriminal gangs 'The Shadow Brokers' and 'The Lazarus Group', affected over than 300,000 computers across more than 150 countries. For the UK's National Health System (NHS) alone, the cost of the attack was estimated in $23 million of lost output (more than 19,000 cancelled appointments) and $89 million in IT costs related with restoring systems and data (Field 2018).

Despite the billions spent for cybersecurity, cyberattacks are still considered the number one risk in Europe, East Asia and the Pacific and North America, i.e., regions that account for 50% of global GDP (World Economic Forum 2018). One of the most susceptible to cybercrime sectors is the travel and tourism sector, with hospitality organizations ranking third in incidents of compromises after retail businesses and financial institutions (Trustwave 2019). The large amounts of online travel bookings predicted to reach $434 million in 2019 and expected to further grow annually by 6.2% to $552million by 2023 (Statista 2019), have always been a point of attraction for cybercriminals. But it appears that what makes the sector more attractive is the customer data that is stored in a multitude of computers, servers and networks of hotels, airlines, booking and car rental companies, even restaurants and bars. According to PwC's Hotels Outlook report 2018-2022 (PwC South Africa 2018:49-53), hotels and hotel groups of all sizes have the second-highest number of data breaches after retail stores. Most international hotel groups from Marriott and Starwood to Wyndham, Intercontinental, Hyatt, Rezidor, Mandarin Oriental and Omni, as well as smaller independent hotels, have fallen prey to cyberattacks several times in the past few years. But also other companies in the sector such as airlines (Air Canada, British Airways, Cathay Pacific, Delta), tour operators (Thomas Cook), travel websites (Expedia, Orbitz, Rail Europe), third-party booking platforms (Sabre Hospitality Solutions), holiday camps (Butlins), travel trade groups (ABTA), restaurant chains (Arby's, Checker and Rally's, Cheddar's) and even bakery-cafés (Panera Bread) to name a few, have been hacked in the last couple of years and many of them not only once.

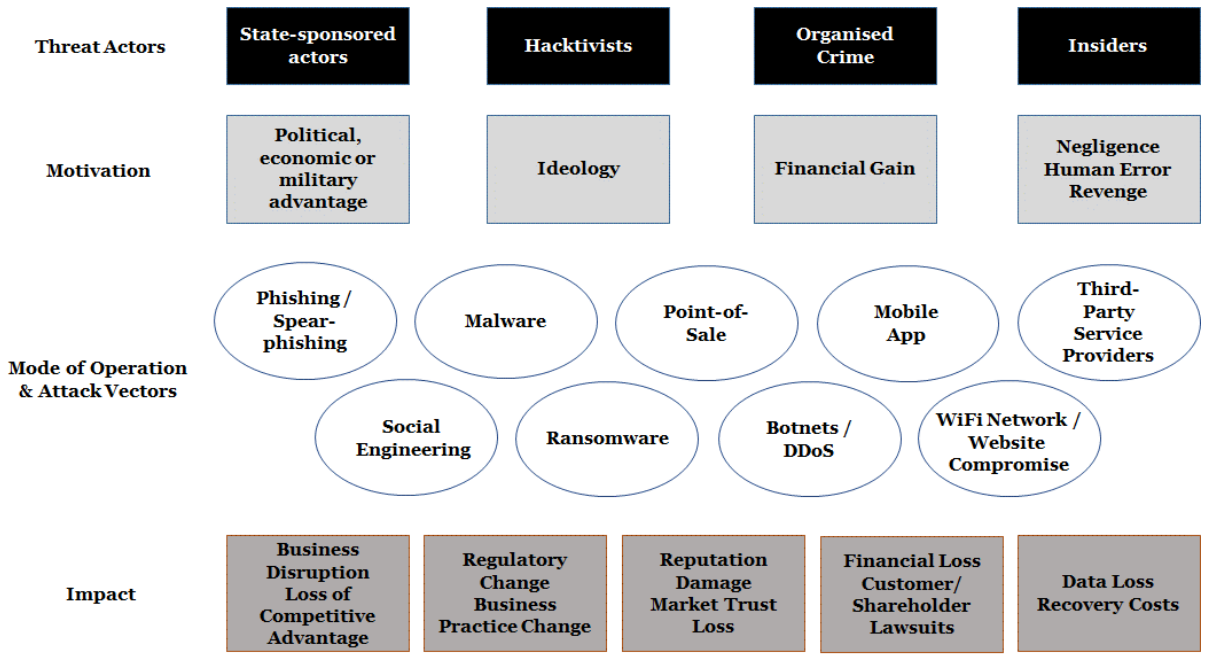
An analysis of the data breaches and attacks appearing in the press shows that the sector is highly vulnerable to cybercrime mainly due to its huge fragmentation, the complexity of the travel booking and payment networks involving numerous agents and third-party service providers, the poor defences of its legacy IT and point-of-sale (POS) systems, the millions of travellers interacting with travel organizations in the cyberspace and human error. Also, many travel and tourism organizations focus their security efforts on meeting compliance obligations, while others start scrutinising their defences only in the aftermath of a breach or after interest from a senior executive. Taking such an ad hoc approach to cybersecurity works briefly in the short-term but leaves the organization exposed to future threats. As a result, even substantial investments on cybersecurity often lead to very low returns. Bone (2017:55) describes the phenomenon of this "endless cycle of massive spending on cybersecurity with no evidence of risk reduction in security" as a "Cyber Paradox". He

argues that this is due to the focus on technology defences and lack of a holistic risk-based view of the cyber threats that organizations face and of their vulnerabilities in their current and future operating environments. Cybersecurity is not just about technology: it involves people and information, systems and processes, culture and physical surroundings. Organizations need to create a secure cyberspace for their employees, partners, suppliers and customers but also need to remain resilient in the event of an attack. To prevent, prepare for and respond to cyber threats by taking a risk-based approach, organizations must be able to give answers to questions on who, why, what and how.

2. Understanding the Cyber Risk Landscape

In his Art of War, Sun Tzu says that "if you know the enemy and know yourself, you need not fear the result of a hundred battles". The first step in a risk-based view of cybersecurity is to understand who these threat actors are, why they do what they do, what they are looking for and how they operate. But as risk is generated at the intersection of a threat with a vulnerability, for organizations to reach a full appreciation of their risk landscape, they must also know themselves. Additionally, they need to be able to identify the internal and external vulnerabilities that threat actors (attackers) can potentially exploit in an attack and the attack vectors (path and means) they will use. Fig. 1 summarises this cyber risk landscape.

Fig. 1 – The Cyber Risk Landscape



2.1. Threat Actors and their Motives

Quite a few threat actor typologies exist with the "Dutch typology" which was developed by the University of Delft in the Netherlands (de Bruijne et al 2017) offering the most sophisticated analysis of eleven actor types alongside their potential targets, expertise, resources, organization and motivation. However, for an organization to understand its cyber risk landscape it is enough to consider that cyberattacks fall broadly under three categories: warfare, activism and crime. Consequently, they can be geopolitically, ideologically and financially motivated and the threat actors behind these categories of attacks can be classified in state-sponsored actors, activists and criminals.

2.1.1. State-sponsored Actors

State-sponsored actors also known as Nation-State APTs (Advanced Persistent Threat groups) are directed, funded and technologically supported by a nation-state and operate to advance that nation's particular interests and political agendas.

In 2015 LOT, the Polish national air carrier was forced to ground its fleet following a cyberattack to its computer systems that were managing flight plans at Warsaw's Okecie Airport (Morgan 2015). This attack was later connected with the approval by the country's president of a very controversial and unpopular surveillance law (BBC News 2016). State-sponsored actors usually steal intellectual property, sensitive personally identifiable information (PII), and money to fund other espionage and exploitation causes (Ablon 2018). Travelling government officials, military personnel, senior corporate executives and research scientists are particularly attractive to these actors, who are interested in every possible information they can collect about them, including information contained in the devices they carry.

The notorious Korean-speaking DarkHotel group exploited vulnerabilities of more than 100 luxury hotel Wi-Fi networks in Asia, Europe and the US to make persons of their interest download malware which appeared as a legitimate software update. They gained access to sensitive government and corporate information of thousands of guests since they were operating unnoticed for seven years (2007-2014). The fact that its victims were all high-ranking officials and executives plus its later connection with the SONY Pictures attack in 2011 indicate that the group is backed by the North Korean government (Palmer 2017).

Hotel Wi-Fi vulnerabilities were also exploited by APT28 or 'Fancy Bear' with suspected links to Russian military intelligence. In 2017 the group obtained password credentials of Western government and business travellers staying in hotels at seven countries in Europe and one in the Middle East in order then to infect their organizational networks back home (Smith and Read 2017).

The Chinese Ministry of State Security and their affiliated group 'Cloud Hopper' are allegedly behind the 2015 Sabre attack (Morris 2019) and the 2018 Marriott/Starwood data breach (Bing 2018).

2.1.2. Activists (Hacktivists)

Activists or hacktivists are threat actors motivated by some political, economic, or social cause, from highlighting human rights abuse to internet copyright infringement and from alerting an organization for its vulnerabilities to declaring online war with people or groups whose ideologies they do not agree with (Ablon 2018).

Hacktivists often act as online whistle-blowers by disseminating ('doxxing') online sensitive or even classified information they obtained through data breaches. Other times they deface their target organizations' websites, i.e., they change completely the website appearance by hacking its hosting infrastructure and replacing the content with their message. However, their most common practice is to render their targets' websites unreachable by overwhelming their networks or computational capacity with more traffic than they can handle causing them to crash (distributed denial-of-service or DDoS attack).

Ghost Squad Hackers, an offshoot of the hacktivist group Anonymous, conducted a DDoS attack in 2016 on the Trump Hotel Collection website forcing it to go offline. They announced that they were targeting Trump's hate-mongering against Muslims and Mexicans (Masters 2016).

2.1.3. Organised Crime Groups and Black Hats

In the crime category, the 'Dutch Typology' distinguishes threat actors in digital robbers (scammers), fraudsters and extortionists, information brokers and crime facilitators. Whether they operate as parts of organised crime groups or as independent black hats, cybercriminals seek to profit primarily from the wealth of data that passes through the travel and tourism networks and are no longer just interested in credit card records. In these networks, they can find passport data, contact details, birth dates, travel plans, air miles, loyalty points and personal preferences of millions of travellers, all of which can be used in a multitude of ways, ranging from fraud to identity theft and extortion. The common denominator for all these actors is that they operate for financial gain by monetising the stolen data, normally in underground black markets of the dark web.

Dream Market, one of the largest dark web markets, lists several vendors selling reward points from over a dozen different airline reward programmes, including Emirates Skywards, SkyMiles, and Asia Miles. In August 2018, a vendor going by the handle @UpInTheAir was selling a minimum of 100,000 points from several reward programmes starting at $884. These points are mostly used to obtain upgrades in hotel stays but, on many occasions, also to redeem points at local retailers through gift cards. Across the three most popular marketplaces in the dark web (Dream Market, Olympus Market and Berlusconi Market) the most listed were Delta SkyMiles and British Airways miles (Bischoff 2018).

Dark web 'travel agents' are reported to sell packages of flights, hotel bookings, car rentals and tours and activities at 30% of their retail value (Seon 2018). These vendors use stolen credit cards or reward points and air miles from hacked traveller accounts to buy travel services which they can offer at a discount to others. Comments on internet forums such as Reddit and Flyertalk detail the stories of many

victims who found their loyalty points had been used to pay for travel services under the names of other people (Bridge 2017).

Another source of revenue for organised crime is passport information. In 2016, more than 47,000 scanned personal documents, including resident registration numbers, digital passport scans, home addresses, bank accounts, phone numbers and family relations records of Asiana Airlines' passengers were 'leaked' on the internet (Park and Lee 2016). Passport data and, in particular, digital passport scans stolen from travel organization servers are often sold in bulk with an average price between $14 and $60 (Sheridan 2018).

2.1.4. Inadvertent and Malicious Insiders

Research has shown, however, that the most dangerous threat actor for cyberattacks is the insiders, i.e., members of staff who do not respond to training and those who create vulnerabilities through mistakes (inadvertent insiders) or disgruntled employees who either collude with external threat actors or carry out the attack themselves (malicious insiders). Sloppy configuration and maintenance of a server at the Pyramid Hotel Group which manages over 90 hotels under different brand affiliations exposed to the wider public (and to threat actors) a vast array of sensitive data of these properties, including hotel employees data, such as full names and usernames, local PC names and addresses, server names and operating system details, cybersecurity policy details, and a variety of other cybersecurity-related information (Winder 2019). High employee turnover in the travel and tourism sector is another reason for security protocols to become vulnerable, if not regularly reviewed.

2.2. Types of Attack and Attack Vectors

Threat actors are using a wide range of techniques and attack vectors to by-pass the cybersecurity measures that organizations have in place to protect their systems and data. The attacks mostly involve high-level technical skills in programming and code generation and, as the examples above indicate, take advantage of the detected network and organizational security vulnerabilities.

2.2.1. Cognitive Hacks

The continuous improvement and sophistication of cybersecurity defence systems have turned most organizations into 'hard targets' prompting many cybercriminals to revise their tactics and focus on a softer target: the human mind. The theory of 'cognitive hacking' was developed in 2002, even if the technique has been around since the beginning of the internet. Unlike the usual technical cyberattacks where threat actors exploit IT systems' vulnerabilities, cognitive hacks are designed in engineering attack vectors to exploit psychological vulnerabilities of people (social engineering) within organizations using deception to manipulate their perception and change their behaviour for the threat actor to bypass security and carry out the attack (Cybenko et al 2002). When it comes to cognitive hacks, the most proven attack vector and by far the 'weapon of choice' of many threat actors is the email.

Phishing has always been the most common type of cyberattack and involves mass-emailing campaigns to organizations attempting to lure employees into downloading attachments with malware or provide access data. Phishing is speculative in nature as it is targeting hundreds of recipients and exploits the weakest human links in the system. A more sophisticated tactic is spear-phishing which is targeting specific members of staff or roles, after sometimes quite elaborate social engineering based on research on their preferences, interests and habits, to convince them that the email originates from a legitimate source.

Targeted travel organizations often receive emails sent by attackers containing links to legitimate-looking websites requesting them to log in to their accounts or to repair a technical issue. In 2017, several travel agencies received emails from that appeared to come from Sabre (including proper logos and names) providing links to a fraudulent Sabre website and asking them to verify their login credentials. Once travel agents logged in, the criminals captured their credentials and then use them to make fraudulent bookings and issue tickets. In the case of Montecito Village Travel alone, they run $25,000 worth of Royal Jordanian airline tickets (Biesiada 2017). Many hotels and guest houses featured on travel website Booking.com have been targeted by phishing emails in 2018, resulting in users of the website being sent emails asking them to provide payment details. Personal information, such as names, addresses, phone numbers, booking reference numbers and dates were included, leading the recipients to believe that the emails were legitimate (Whitehead 2018).

Phishing, spear-fishing and other cognitive hacking techniques facilitate several other types of cyberattacks which give threat actors access to the organization's systems and networks.

2.2.2. Malware Attacks

Perhaps the most traditional attack method, malware attack compromises an organization's sensitive systems and data by infecting them with malicious software such as viruses, worms, Trojan horses, keyloggers and other spyware. These attacks normally feature the use of a command-and-control server which enables threat actors to communicate with the infected systems, exfiltrate sensitive data and even remotely control the compromised device or server. There are thousands of different malware variants which, once they infiltrate systems and hardware, they spread to other systems leaving a trail of disruption and destruction. IBM's X-Force Incident Response and Intelligence Services (IRIS) teams helped organizations with 200% more destructive malware cases in the first half of 2019 compared with the second half of 2018 and report that organizations hit with destructive malware can experience a total cost of $200 million and lose more than 12,000 devices in an attack (Sheridan 2019).

The most common for the travel and tourism sector malware attack is the 'Carbanak/Anunak attack' (named after the criminal groups that designed it) which uses a spear-phishing tactic. The attacker calls the organization's reservations office saying that they are unable to use the online reservation system and requests to send their information to the agent via email. The attacker stays on the line until the agent opens the attachment contained in the email and hangs up when the attack is

confirmed as successful. The email attachment is normally a Word document that contains malware capable of stealing system information, desktop screenshots, and to download additional network mapping malware (reconnaissance tools). This malware enables remote desktop, steals local passwords, search user's email, target payment systems or install completely different remote desktop programmes and targets credit card data by scraping memory on Point-of-Sale systems (Trustwave 2016).

Another malware attack using the spear-phishing technique is when attackers use a Word document from the travel organization itself (e.g., forms authorising credit card charges in advance of a stay, menu selection in special events, etc.). The document is usually enclosed as part of a self-extracting file, which also installs two other files on the targeted network — one of them a disguised installer for backdoor malware and the other with a script that both opens the Word document and launches the backdoor (Gallagher 2016).

2.2.3. POS (Endpoint) Attacks

Point-of-sale (POS) attacks are a type of malware attack which is very common in the travel and tourism sector and gives threat actors valuable data including credit card information such as card numbers and personal identification numbers (PINs). As mentioned earlier in the chapter, numerous hotel groups (InterContinental, Mandarin Oriental, Radisson) and restaurant chains Arby's, Checker and Rally's, Cheddar's) have experienced data breaches most of which were through their POS systems. According to Verizon (2018), for hotels and restaurants alone, point-of-sale intrusion accounts for 90% of all data breaches.

Memory scraping through malware infection is the most used method to target POS systems with over twenty known types of RAM-scraping malware designed for this purpose. Threat actors take advantage of the lack of security vigilance in the sector during slow periods to attack POS networks. Legacy systems with computers and terminals that have not been updated with the latest security patches or are completely outdated are still used in many hotels, restaurants, pool and beach bars are another easy target for attackers to infect with their malware. The malware can spread itself throughout the organization, eventually infecting all its POS terminals. When a card is swiped, its details are briefly stored in the POS terminal's RAM while being transmitted to the payment processor. The malware installed in the terminal copies the card data and it transmits back to the threat actors normally via an internal staging server, as the POS system is unlikely to have external network access.

There are a variety of methods attackers can use to gain access to an organization's network. They usually look for vulnerabilities in external-facing systems such as using an SQL injection on a web server or finding a computer in the network that still uses the default manufacturer password. Alternatively, they can identify and use an inadvertent insider within the organization through a spear-fishing campaign or a vulnerability among its digital partners and third-party service providers, what is otherwise known as 'Digital Extended Enterprise' or 'DexteR' (Pulkkinen 2018). In 2016, the Russian cybercriminal group Carbanak breached a system support portal

used by Oracle to remotely access and service MICROS point-of-sale systems, gaining the potential to remotely access and infect with malware the MICROS terminals in some 200,000 food and beverage outlets, 100,000 retail sites, and more than 30,000 hotels (Krebs 2016). More recently, a new security flaw in Oracle was found making it possible for threat actors to remotely install POS malware to MICROS terminals (Brooks 2018).

Another endpoint target in the sector is the range of mobile travel apps which are becoming increasingly popular also among treat actors. Air Canada (2018), for example, reported that following 'unusual login behaviour' it decided to lock all passengers' mobile accounts until they update their passwords, as it suspected that 20,000 of its mobile app users' personal data might have been compromised in a breach. Insecure data storage within the app alongside insecure inter-process communication and often unwarranted data transmission can potentially enable attackers to remotely access data processed within the app (Positive Technologies 2019). Skyscanner, TripAdvisor and Kayak mobile apps were found to be sending personal data to Facebook without users' consent (Taylor 2019). Apart from breaking General Data Protection Regulation (GDPR) rules which require the explicit consent of users before personal information is collected or shared, the transmission of data was done with built-in Facebook trackers that could be intercepted by any threat actor.

2.2.4. Ransomware Attacks

A very different type of malware attack is the ransomware attack. The goal of this attack is not to steal data but to deny its owner access to it. While other types of malware attacks are more complex for the threat actors to monetise (e.g., stolen data needs to be exfiltrated, bundled and sold in dark web forums and markets), the objective of a ransomware attack is to make the target pay the attacker directly. The ransomware is programmed to identify the organization's most sensitive or valuable data, corrupt the backups to make them useless, create backdoors in the system for easier future infiltrations, encrypt the data and then send to the target a ransom demand, usually to be paid in cryptocurrency. To make their demands more compelling, threat actors often incorporate wiper elements into their attacks, such as with new strains of ransomware like LockerGoga and MegaCortex, resulting in a spike of 116% of calls to X-Force IRIS' teams for ransomware incidents in the first half of 2019 (Sheridan 2019). Usually targeted organizations do not disclose such attacks or, if they do, they deny that they have paid any ransom. However, as the ransomware variants employed are rather unpredictable and often difficult to defend against, many organizations resort in buying cyber-insurance and stockpiling cryptocurrencies for ransom payment (Wall 2018). Citrix reports that more UK-based companies are now building a ready stockpile of cryptocurrency for a ransomware attack, rising from 33% in 2016 to 42% in 2018 (Mayers 2018).

Ransomware attacks have become very common in the travel and tourism sector with targets ranging from the Louisville Regional Airport Authority in Kentucky, USA and the Bristol Airport in UK to the Bin Line and Goldjoy travel agencies in Hong Kong and from Marriott/Starwood hotel group worldwide to The Piccadilly Hotel in Lucknow, India to name a few that have been reported to the press. Notably,

ransomware attacks do not target only data but also operating systems as evidenced in the attack of the Romantik Seehotel Jaegerwirt in the Austrian Alps. The attackers infiltrated the hotel's electronic key system locking hotel guests in their rooms and locking the hotel out of its systems thus disabling staff to issue new key cards to guests. They demanded a ransom of two Bitcoins and warned that the cost would double if the hotel did not comply with the demand by the end of the day (Bilefsky 2017).

2.2.5. Botnet / DDoS Attacks

Botnet attacks use networks of thousands and even millions of computers, smartphones, or intelligent devices (botnets or 'zombie armies') for malicious login attempts, mass spam attacks or to take down a network, network devices, websites or an organization's IT environment. These computers have been infected with malware, enslaving them to be commanded by the threat actors who infected them to provide the raw computing power to launch botnet attacks. Once an attack is initiated, botnets are used to send vast quantities of requests /enquiries ranging from simple ping messages to bulk email messages. The huge volume of incoming traffic overwhelms the targeted network/server or website to the point that other legitimate users are unable to access it or that it crashes. The objective of such attacks is to disrupt normal working operations or degrade the overall service of the target organization and this is the reason why they are also known as Distributed-Denial-of-Service (DDoS) attacks. In May 2018, the Danish Railway experienced a powerful DDoS attack causing the app, the website and the ticket system to crash. The organization's email and telephone servers went also down causing both a transport and communication chaos in Denmark (Hill 2018). Airlines are also a common DDoS attack target with the severity of attacks increasing dramatically in recent years and many airline IT outages attributed to them (Elliott 2019).

The threat actors' motivation for a DDoS attack can be political or ideological (like the Ghost Squad attack on the Trump Hotel Collection website discussed earlier) as well as financial. When it comes to financial gains, the threat actor asks for money directly from the target just like in ransomware situations or may be paid by a third party, usually a competitor or a disgruntled employee. DDoS-for-hire services are offered by the hour for $10 and by the day at bulk discount rates of $200 (Wilczek 2019).

Akamai Technologies (2018) analysed 112 billion bot requests and 3.9 billion malicious login attempts between November 2017 and April 2018 against sites belonging to airlines, cruise lines, hotels, online travel, automotive rental and transport organizations and reported that cruise lines are the target of twice as many botnet attacks than those connecting to airline and hotel sites with 50 billion events that targeted the cruise industry alone. According to the report, these attacks originated predominantly from China and Russia with attacks being three times the number of attacks originating from the US and Indonesia (third and fourth attack origins respectively).

Travel websites are attacked by scraping botnets querying for any ticket they can sell, skewing look-to-book ratios, increasing GDS transaction costs, and causing website

slowdowns and downtime. Threat actors dynamically package hotel room and airline seat inventory with other products, stealing direct and ancillary revenue.

2.2.6. Attacks on Third-party Service Providers

Threat actors also target members of the organization's 'DexteR' (digital partners and third-party service providers). According to the 2018 IBM X-Force Threat Intelligence Index, more two-thirds of total data records compromised in 2017 were the result of organizations' insiders. Attackers deliberately targeted employees and managers, partners and third-party service providers who are often the 'weaker links' in the network as well as attractive aggregation points for sensitive organizational data (IBM 2018).

An example of organised crime taking advantage of third-party vulnerabilities and organizational slack and of turning both third-party and the organization's IT team to 'inadvertent insiders', is the 2018 British Airways data breach. The cybercriminal group Magecart managed to identify and inject malicious code to a third-party piece of Javascript which was unchecked and for a long time not updated by the British Airways IT team. The infected script enabled payment details of about 380,000 passengers to be diverted to the fake website 'baways.com' - developed and controlled by Magecart - as they were entered by these passengers (Stokel-Walker 2019). Similarly, in April 2018, Delta airlines announced that payment card information of several hundred thousand passengers might have been exposed by a malware breach in software provided by (24)7.ai, a third-party supplier which provided solutions for online chat, virtual agents and customer analytics (Delta 2018).

Websites hosting and outsourced service providers are also commonly targeted 'DexteR' nodes. The Association of British Travel Agents (ABTA) found out in February 2017 that its web server which was managed through a third-party hosting company was compromised exposing data of 43,000 individuals, travel agents and tour operators. The breach also exposed PII of roughly 1,000 holidaymakers who have made a complaint about an ABTA-registered travel agent. Cybercriminals targeted in 2017 Sabre's SynXis hospitality reservation system even if, in the end, only a limited subset of reservations processed through the system were viewed and attackers did not access customers' personal information. SynXis was a lucrative target because it was handling, at the time, bookings for around 35,000 hotels under more than a dozen different brands (Sabre 2017).

2.2.7. Wi-Fi Network / Website Compromise

Threat actors also take advantage of unsecured public networks in hotels, cafés, airports and visitor attractions to infiltrate traveller devices, infect them with malware and either steal their personal data or use them as inadvertent insiders for other targets.

Apart from attacks using Wi-Fi vulnerabilities like the DarkHotel group described earlier, threat actors use also a technique known as the 'evil twin' attack. They position themselves near an authentic Wi-Fi access point (e.g., a museum's public Wi-Fi network) and discover its service set identifier (SSID) and frequency. They

then send a radio signal using the exact same frequency and SSID which to the other museum visitors appears as the legitimate hotspot with the same name. When visitors connect to the evil twin, threat actors take control of their device, collect their personal data and can monitor every activity performed in the device. Evil twins are historically known as honeypots or base station clones and are one of the most common cyber threats in the travel and tourism sector (McCue 2019).

Travel and tourism organizations' websites are another attack vector for stealing valuable customer data, including PII and payment details. Research (Greif 2018; Wueest 2019) has shown that major airline and hotel websites leak detailed guest booking data (including booking reference code, full name, address, mobile phone number, passport number, and the last four digits of credit card numbers) to third-party advertisers, social media websites, data aggregators, and other partners. Some websites leak guest information to online partners during the booking process itself, while others leaked it when customers logged in to their reservation page. Threat actors can access and use this data to log into a reservation, view personal details, and even alter or cancel the booking.

3. Building Cybersecurity Capability

Already from 2010, Dmitri Alperovitch, McAfee Vice President of Threat Research, when he revealed a five-year cyberattack that hit 14 countries, tagged as "Operation Shady RAT", has said that *"the only companies not at risk are those who have nothing worth taking"*. His report concluded that there are two kinds of companies today, *"those that know they have been compromised, and those that still haven't yet realized they have been compromised"* (Bright, 2011). The number of cyberattacks over the last 5 years is evidence enough to show that travel and tourism organizations, regardless of their size, have data worth taking and are still an easy target for threat actors. For any organization in the sector it is not a matter of 'if' but a matter of 'when' and, therefore, they must take a business-led and risk-based approach to build cybersecurity capability to defend themselves from all these types of cyberattacks and more. Again, answers to the questions who, what, why and how need to guide the planning

3.1. Cybersecurity Governance

In many organizations, cybersecurity is an issue that concerns the IT department and the Chief Information Security Officer (CISO), if such a role exists, and the focus of their strategy is mere compliance to the legislative and regulatory requirements. However, as already discussed, data breaches have become causes for class-actions against the senior management of companies (directors and officers), as the examples of Wyndham's shareholder lawsuit in 2014, the securities lawsuit against the China-based Huazhu Hotel Group (LaCroix 2018) and the Marriott class-action in 2018 (Cision 2019) have already shown, notwithstanding the wave of class-actions expected against British Airways (Schwartz 2018) and other high-profile companies in the sector.

Cybersecurity today requires leadership from the board and senior management that goes beyond the approval of new IT investments and compliance with security regulations. Rather, boards and senior management must first see cyber as an organization-wide issue and expect everyone to be accountable for managing the risk and, second, assume cybersecurity oversight just as they do with any other significant risk to the organization and consider.

This can be achieved either with the entire board overseeing cyber risk or by delegating this oversight to a board committee, normally the Audit Committee or a committee headed by a director with a technology or cybersecurity background that will provide the board with regular and comprehensive updates. Where such knowledge does not exist within a Board, it should be acquired, just like Marriott International did with the appointment as an independent director of Margaret M. McCarthy, Executive Vice President at CVS Health Corporation, specifically for her experience and knowledge of privacy and cybersecurity (Marriott 2019). This appointment sent all the right signals to stakeholders that cyber has become a serious item in the C-suite agenda in the aftermath of the massive data breach it experienced in 2018.

3.2. Setting Priorities: What Matters Most?

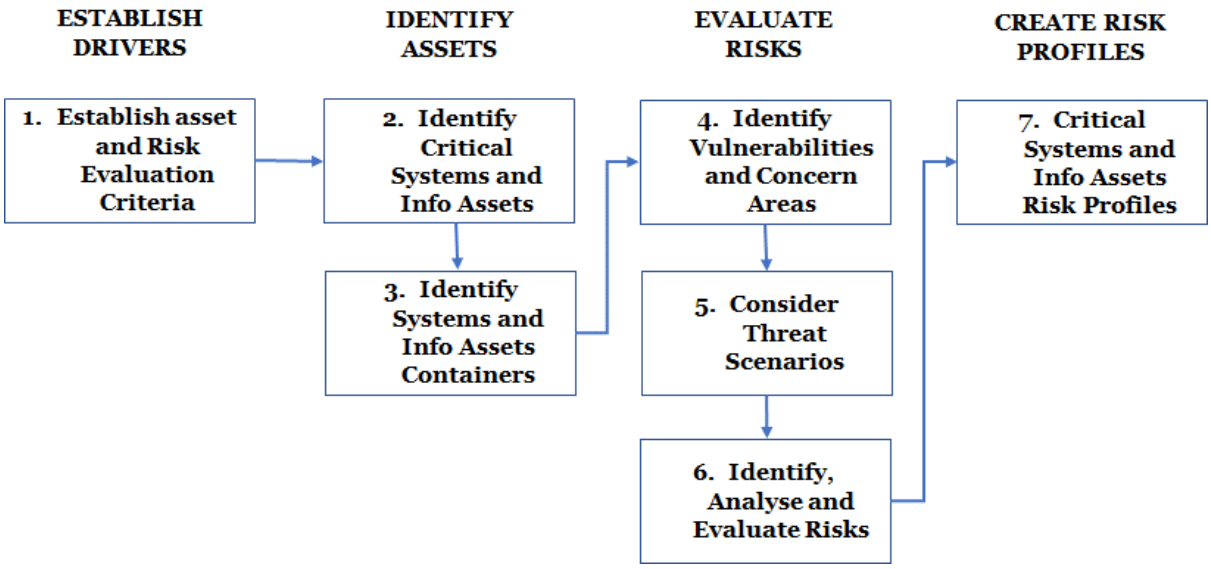
A cybersecurity strategy that provides the best protection to key business assets and operations, requires the organization to understand what IT systems are mission-critical for its operation as well as what information assets are of value to threat actors and then provide these with enhanced protection. This means knowing not only which are these systems and assets, but where they are located and who has access to them. It also means understanding how these assets are related to each other, what are the possible threats to them and what vulnerabilities (both organizational and technological) can expose them to threat actors.

The result of this activity, which is also referred to as the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) methodology to information security risks (Alberts and Dorofee 2002), is a set of critical system and information asset risk profiles (Fig. 2). These profiles will enable decision making about resource allocation to strengthen the cyber-defences of the organization and the development of a cybersecurity strategy for their protection.

3.3. Cybersecurity Strategy, Mechanisms and Controls

The cyber-protection strategy should inform organizational policies and standards covering three main areas: the organization's human element, likelihood management and consequence management.

Fig.2 – Critical System and Information Asset Risk Profiling



Adapted from: Alberts and Dorofee (2002)

3.3.1. The Human Element

As discussed earlier in the chapter, cybersecurity is not only about technical defences because the human element, inadvertent and malicious insiders (employees, business partners and third-party vendors) account for the largest part of system outages and data breaches. In many cases, the disconnect of the human element from sound cybersecurity practice comes down to how organizations engage their employees and generate awareness through their communications and training programmes. One-size-fits-all programmes are generally ineffective; therefore, they must be tailored to the organization, aligned with its operational goals and fit-for-purpose for specific audiences. Training must be customised based on the trainees' physical and network access levels, their privilege rights, and their job responsibilities and focus on the specific threats, challenges, and responsibilities for each position (i.e., the reservation agents' curriculum will be different from the one for the finance staff and from that for third-party vendors).

Policies and standards should define the organization's and its 'DexteR' behavioural expectations with regards to information management and IT systems' usage and maintenance (e.g., administrative access, password policies, social media, removable media, reporting incidents, BYOD, etc.) and communicate the consequences for any violation of those.

3.3.2. Likelihood Management

The second dimension of a cybersecurity strategy is the reduction of vulnerabilities in an organization's digital ecosystem through enhancement of defences and measures that are proactively put in place to deter threat actors from attacking it. Decisions need to be made and detailed standard operating procedures to be developed on key 'cyber hygiene' issues such as, for example, systems' physical security, identity and access management, third-party and external dependencies, network segmentation, malware and patch management and information protection and encryption. It may appear counter-intuitive, but travel and tourism organizations still have problems with basic cyber hygiene issues such as access management. For example, according to a Dashlane study (Katz 2018), 89% of travel-related sites leave their users' accounts exposed to cybercriminals due to unsafe password practices. Of the 55 travel websites tested only Airbnb received full marks whereas large organizations such as American Airlines, Carnival and Norwegian Cruise Lines failed the test.

As endpoints (POS, websites, BYOD, servers) are usual targets of cyberattacks, robust preventive and detective capabilities must be developed at the endpoints themselves to provide a layer beyond the network-centric IT security defences. Endpoint security suites today include a variety of tools beyond simple antivirus software and application firewalls and include Intrusion Detection/Protection Systems (IDS/IPS) and Data Leakage Protection (DLP) solutions and other security and incident/event monitoring mechanisms. The critical system and information asset profiling will enable decisions on whether this level of endpoint security is sufficient or if the organization needs to move to 'next generation' ('next-gen') endpoint security. Often traditional IDS/IPS do not offer an adequate defence mechanism. In November 2018, Radisson Rewards global loyalty programme notified the public about a data breach which occurred in early September and identified almost 20 days after its occurrence. Some reports on the breach suggested that the hotel group's intrusion detection capability was limited (Ashford 2018). 'Next-gen' endpoint security involves system behavioural analysis mechanisms for abnormal software behaviour, traffic detection systems that recognize and block the communication from a an infected file to the threat actor (e.g., notifying the actor that the file has successfully infiltrated the system), and exploit mitigation mechanisms that recognize thereat actors' scripts and block them.

3.3.3. Consequence Management

The third dimension of a cybersecurity strategy is about the response of the organization in the advent of an attack or a data breach. The organization must develop a three-pronged crisis management plan which defines escalation and prioritization processes to manage and coordinate IT, operational, and systems' recovery issues related with a cyberattack and covers incident response, business continuity and crisis communications. A multifunctional crisis management team which, depending on the incident severity may include C-suite members, co-ordinates all three aspects of the plan but dedicated expert teams should normally be allocated for each one of these aspects.

Incident response concerns the cyber-attack itself (e.g., DDoS or ransomware attack) and the team responsible for this must have substantial relevant expertise to address all the technical and other challenges, such as negotiations with the threat actors, the organization faces as a consequence of the incident. The team members must also possess technical forensic and investigative skills that are vital to preserving evidence and analysing possible control failures, security lapses, and other conditions related to the incident. Incident response often requires the engagement of external help in the form of 'white hats', cybersecurity consultants that can bring to the organization specialist expertise required to deal with the incident and the investigation that will follow in its aftermath.

The team dedicated to business continuity can be also part of the incident response team. The focus of this team is for the organization to maintain its operational capability during an incident through the protection of mission-critical systems or the deployment of back-up systems. The team will also be involved in the recovery of systems that failed or were damaged as a result of the attack and help in the strengthening of the network security, the improvement of protocols and the enhancement of vigilance after the incident.

The crisis communications team is the one who ensures accurate and timely flows of information between the crisis teams internally and the organization and its stakeholders externally. Back in 2015, Mandarin Oriental handled very poorly the malware attack on their credit card systems which affected 2,850 California-based guests. The hotel group admitted the attack in March 2015 and posted a notification in its website just acknowledging that the breach started in June 2014 but not providing any further information except that they had no evidence of misuse of the data. However, cybersecurity researchers had already reported "about a pattern of fraudulent charges on customer cards that had all recently been used at Mandarin hotels" (Krebs 2015). The group did not notify any of the potentially affected guests at the time of the notification and it was highly unlikely that guests that stayed in their hotels since the previous June would check the website at all. Mandarin officially reported the incident to the California authorities and started sending notices to the affected guests on July 10, 2015.

In the US, regulation for reporting breaches is different from the EU's GDPR and organizations have more time to prepare their response before informing potentially affected customers and the wider public. GDPR states a maximum time of 72 hours for reporting, therefore Radisson Rewards' data breach reporting which was late 20 days will be an interesting test case (Ashford 2018). Marriott, on the other hand, had the time to prepare a comprehensive communications strategy that was rolled out together with its data breach reporting (Table 1).

Table 1 – Marriott/Starwood 2018 Data Breach Communication Strategy

Public reporting	Public notice of the incident via a press release and notification banners across Marriott's websites and the Marriott and Starwood Preferred Guest apps.

E-mail notifications	E-mail notifications on a rolling basis to guests who had valid email addresses in the affected databases.
Dedicated Website	Dedicated website to provide information and updates about the incident in 20 languages. Information about how potentially affected guests can monitor and protect their data and details on web monitoring services.
Dedicated Call centres	Dedicated call centres most of which operated seven days per week, to answer guests' questions about the incident, multiple languages. Through February 28, 2019, the call centres had received approx. 53,000 calls with average wait time in the United States and Canada nine seconds.
Credit / Personal Data Monitoring Service	Two free monitoring solutions for potentially affected guests: 1. WebWatcher for US, UK and Canadian guests, offering also fraud loss reimbursement coverage and unlimited fraud consultation services for one year. 2. Experian for other countries with their IdentityWorks Global Internet Surveillance product Through February 28, 2019, approx. 250,750 guests had activated WebWatcher and 36,000 guests had enrolled with Experian.
Claims Processing	A process for guests to submit individual claims of fraud related to this incident.

Source: Schaal (2012)

Apart from the crisis management plan, a useful reactive measure for a cyberattack is a cyber-insurance policy. Although many organizations are reluctant to buy such a cover, cyber-policies pay out despite the claim complexities an organization may have to navigate. Marriott announced in March 2019 that the 2018 data breach had costed the company, pre-tax, a total of $28 million, but those expenses were offset by insurance recoveries of approximately $25 million (Olson 2019). Normally, the organization will liaise with a specialist insurer or broker for a cyber-policy and will get the opportunity to explore potential loss scenarios, gain a better understanding of how a proposed coverage might respond in each of those scenarios and then make any adjustments are deemed necessary. Cyber-insurance policies also offer access to expert consultancy and support on how to manage the technical, legal and reputational consequences of a cyberattack.

3.4. Systems' Testing and Reviewing

The last step in building cybersecurity capability is the design of a process that ensures that cybersecurity policy, standards, systems, measures and tools are consistently and effectively used and regularly updated. To assess and benchmark

the effectiveness of its cybersecurity strategy the organization must develop audits with actionable metrics and key performance indicators (KPIs) focusing on the degree of compliance with internal and external standards; financial impact of incidents; key security projects/initiatives (status vs target and progress vs plan); cybersecurity culture (measuring clarity of rules, practicability, visibility, staff engagement, organizational and peer openness, exemplary behaviour and enforcement); and overall cybersecurity maturity level (KPMG 2015).

The robustness of the organization's cybersecurity defence mechanisms can be evaluated with penetration testing ('pen testing') in which internal or external penetration testers attempt to gain root access or other privileged control over an organizations system, Wi-Fi network, website, mobile application or devices that could be stolen and access to sensitive data. These tests facilitate the identification of systems' vulnerabilities and configuration issues before a thereat actor exploits them (Maxwell 2019).

'Red teaming' exercises assess the cyber readiness and awareness of the organization through customized scenario-based incident simulations. These simulations enable the various 'blue' teams (incident response, business continuity, communications and crisis management team) to rehearse the crisis management plans for a realistic cyber incident within a safe learning environment. Red teaming exercises increase awareness of cyber threats, raise understanding of how varied and complex they can be and improve understanding of roles, responsibilities and decisions required in response to a cybersecurity incident (Maxwell 2019). They also offer a unique opportunity to engage management at a C-suite level in the wider context of cyber threats including issues with regards to human capital, technology capabilities and limitations, legal and jurisdictional challenges, crisis communications, stakeholder engagement, media, customer and external affairs.

In a dynamic environment where threat levels, actors and attack vectors are constantly evolving, audits and tests run regularly, and their findings and outcomes must inform updates and revisions of the organization's cybersecurity strategy.

4. Future Cybersecurity Developments in Travel and Tourism

The future travel and tourism cyber-ecosystem will increasingly adopt new and disruptive technologies to provide anytime and anywhere access. It will use automation, virtualization, software-defined networks and hybrid data centres and organizations in the sector will be required by their markets to architect more flexible operationally secure environments. Many high-profile organizations in the sector made the headlines over the last few years because they did not pay this second requirement the attention that was needed.

Although admittedly, the awareness of cyber threats among organizations in the sector is on the rise, threat actors are finding new and creative ways to achieve their objectives. For instance they use legitimate file-sharing and questionnaire-hosting services from trusted companies to avoid the blocking of their phishing attacks or

using takeaway restaurant websites as 'watering holes' to plant malware to organizations' networks when their employees browse the menu from their secure devices (Kaushik 2019). As the threat landscape continues to grow, traditional cybersecurity strategies and tools are gradually becoming ineffective. People, processes, and technology have no option but to evolve so that they can support the new enhanced security needs. The cybersecurity mindset in these organizations will have to shift from reactive to proactive. So, instead of merely detecting malware and attack vectors 20 or 50 days after they were installed and when they have already caused damage, they will proactively search for malware and attackers that are lurking in their networks before they are activated. This 'threat hunting' approach (Kumar 2019) is the new strategy in cybersecurity which is now facilitated with advanced Endpoint Detection and Response (EDR) solutions and AI technologies.

With so many security failures and breaches reported in the press, data protection and privacy will become one of the sector's competitive differentiators. Organizations which treat this aspect just as a compliance exercise will eventually lose the trust of the market. However, identity and access management will be seen more from a customer perspective, and therefore inevitably, travel and tourism organizations will look for solutions that offer them flexibility and adopt more the as-a-service delivery models (e.g., IDaaS, PAMaaS, etc) that offer passwordless authentication, single sign-on and user-friendly multi-factor biometric authentication (Gopalakrishnan 2019).

Finally, as more organizations in the sector move their IT infrastructure and data centres to the cloud, the adoption of a 'multi-cloud approach' for distributed reservations, yield and revenue management, channel/distribution management, call centres, and content management are becoming more mainstream because it offers flexibility, resilience and significant cost benefits (Hertzfeld 2019). However, the use of multiple clouds increases the complexity of securely managing systems and information assets and the likelihood of dis-jointed visibility and inconsistent application of cybersecurity controls (Joseph 2019). The two main challenges for travel and tourism organizations will be, first, to ensure PCI compliance when personally identifiable data traverses multiple cloud boundaries and, second, to devise an integrated threat prevention strategy and automated threat detection and response.

References:

Ablon L (2018) Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data. The RAND Corporation https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf. Accessed 30 May 2019

Air Canada (2018) Notice to Air Canada mobile app users https://www.aircanada.com/ca/en/aco/home/book/travel-news-and-updates/2018/notice-air-canada-mobile-app-users.html. Accessed 22 July 2019

Akamai Technologies (2018) Summer 2018 - State of the internet/security: web attack, https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/soti-summer-2018-web-attack-report.pdf. Accessed 25 July 2019

Alberts CJ and Dorofee A (2002) Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co Inc, Boston Massachusetts

Ashford W (2018) Radisson hotel group could be GDPR test case. Computer Weekly, 2 November https://www.computerweekly.com/news/252451870/Radisson-hotel-group-could-be-GDPR-test-case. Accessed 24 July 2019

BBC News (2016) Poland surveillance law approved by president. BBC News, 5 February https://www.bbc.co.uk/news/world-europe-35501677. Accessed 14 May 2019

Biesiada J (2017) How to not fall victim to fraud. Travel Weekly, 22 September https://www.travelweekly.com/Travel-News/Travel-Agent-Issues/Insights/Ways-to-not-fall-victim-to-fraud. Accessed 23 July 2019

Bilefsky D (2017) Hackers use new tactic at Austrian hotel: locking the doors. New York Times, 30 January https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html. Accessed 24 June 2019

Bing C (2018) Exclusive: Clues in Marriott hack implicate China. Reuters, 6 December https://www.reuters.com/article/us-marriott-intnl-cyber-china-exclusive/exclusive-clues-in-marriott-hack-implicate-china-sources-idUSKBN1O504D. Accessed 7 July 2019

Bischoff P (2018) How much are stolen frequent flyer miles worth on the dark web? Comparitech https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/. Accessed 22 July 2019

Bone J (2017) Cognitive hack: The new battleground in cybersecurity... the human mind. Auerbach Publications, New York

Bridge M (2017) Russians buy life of luxury with stolen UK air miles. The Times, 21 November https://www.thetimes.co.uk/edition/news/russians-buy-life-of-luxury-with-stolen-uk-air-miles-psrkhqsfs. Accessed 23 May 2019

Bright P (2011) “Operation Shady RAT”: five-year hack attack hit 14 countries. Ars Technica, 3 August https://arstechnica.com/information-technology/2011/08/operation-shady-rat-five-year-hack-attack-hit-14-countries/. Accessed 30 May 2019

Brook C (2018) Vulnerability affects oracle MICROS POS systems, business data. Digital Guardian, 1 February https://digitalguardian.com/blog/vulnerability-affects-oracle-micros-pos-systems-business-data. Accessed 2 June 2019

Cision (2019) Pierce Bainbridge files class action on behalf of travelers worldwide in the Marriott data breach, 11 February https://www.prnewswire.com/news-releases/pierce-bainbridge-files-class-action-on-behalf-of-travelers-worldwide-in-the-marriott-data-breach-300793327.html. Accessed 12 June 2019

Cybenko G, Giani A and Thompson P (2002) Cognitive hacking: A battle for the mind. Computer 35(8):50-56

de Bruijne M, van Eeten M, Gañán CH and Pieters W (2017) Towards a new cyber threat actor typology. Delft University of Technology https://www.wodc.nl/binaries/2740_Volledige_Tekst_tcm28-273243.pdf. Accessed 28 June 2019

Delta (2018) Statement on [24]7.ai cyber incident https://news.delta.com/updated-statement-247ai-cyber-incident. Accessed 28 May 2019

Elliott C (2019) Hackers are targeting airlines in record numbers. Here's what that means for you. Forbes, 25 February https://www.forbes.com/sites/christopherelliott/2019/02/25/hackers-are-targeting-airlines-in-record-numbers-heres-what-that-means-for-you/. Accessed 22 May 2019

Field M (2018) WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled. The Telegraph, 11 October https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/. Accessed 3 May 2019

Gallagher S (2016) Checking in with spear phishing, criminals check out with hotel credit card data. Ars Technica, 5 October https://arstechnica.com/information-technology/2016/05/hotels-face-increasingly-targeted-attacks-on-customer-data/ Accessed 30 May 2019

Gartner Inc (2018) Gartner forecasts worldwide information security spending to exceed $124 billion in 2019 https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. Accessed 18 August 2018
Gopalakrishnan C (2019) Biometrics gaining ground as a password alternative. SC Magazine, 25 July https://www.scmagazineuk.com/biometrics-gaining-ground-password-alternative/article/1592139. Accessed 25 July 2019

Greif B (2018) Lufthansa data leak: what a single URL can reveal about you. CliqZ Magazine, 29 August https://cliqz.com/en/magazine/lufthansa-data-leak-what-a-single-url-can-reveal-about-you. Accessed 23 July 2019

Hertzfeld E (2019) G6 Hospitality upgrades to advanced tech platform. Hotel Management, 23 May https://www.hotelmanagement.net/tech/g6-hospitality-upgrades-to-advanced-hospitality-tech-platform. Accessed 22 July 2019

Hill M (2018) Danish railway company DSB suffers DDoS attack. InfoSecurity Magazine, 14 May https://www.infosecurity-magazine.com/news/danish-railway-ddos-attack/. Accessed 26 May 2019

IBM (2018) 2018 IBM X-Force Threat Intelligence Index https://www.ibm.com/security/security-intelligence/qradar/insider-threat. Accessed 15 May 2019

Joseph A (2019) How to address the multi-cloud security conundrum. CSO Online, 5 August https://www.cso.com.au/article/664942/how-address-multi-cloud-security-conundrum/. Accessed 7 August 2019

Kaspersky Lab (2018) Damage control: the cost of security breaches https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf. Accessed 22 July 2019

Katz E (2018) 2018 Travel Website Password Power Rankings. Dashlane Blog, 2 May https://blog.dashlane.com/travel-password-power-rankings-2018/. Accessed 12 June 2019

Kaushik S (2019) Cyberspace danger: can we really prevent internet fraud? Financial Express, 29 April https://www.financialexpress.com/opinion/cyberspace-danger-can-we-really-prevent-internet-fraud/1561909/, Accessed 15 May 2019

KPMG (2015) FEEL FREE Cyber Security Dashboard http://kpmg.co.uk.s3-website-eu-west-1.amazonaws.com/email/06Jun14/OM020788A/index.html. Accessed 15 May 2019

Krebs B (2015) Credit Card Breach at Mandarin Oriental. KrebsOnSecurity, 4 March https://krebsonsecurity.com/2015/03/credit-card-breach-at-mandarian-oriental/. Accessed 15 June 2019

Krebs B (2016) Data breach at Oracle's MICROS point-of-sale division. KrebsOnSecurity, 8 August https://krebsonsecurity.com/2016/08/data-breach-at-oracles-micros-point-of-sale-division/. Accessed 15 June 2019

Kumar A (2019) F-Secure talks up threat-hunting to stay ahead of cyberattacks in APAC. Computer Weekly, 25 July https://www.computerweekly.com/news/252467332/F-Secure-talks-up-threat-hunting-to-stay-ahead-of-cyber-attacks-in-APAC. Accessed 31 July 2019

LaCroix K (2018) Chinese hotel company hit with data breach-related securities suit. The D&O Diary, 9 October https://www.dandodiary.com/2018/10/articles/securities-litigation/chinese-hotel-company-hit-data-breach-related-securities-suit/. Accessed 15 June 2019

Marriott International (2019) Marriott International appoints Margaret McCarthy to board of directors. 20 March https://news.marriott.com/2019/03/marriott-international-appoints-margaret-mccarthy-to-board-of-directors/ Accessed 14 June 2019

Mayers C (2018) Ransomware in the UK: one year on. Citrix, 26 February https://www.citrix.com/blogs/2017/06/06/ransomware-in-the-uk-one-year-on/. Accessed 14 June 2019

Maxwell M (2019) How breach and attack simulation (BAS) can help businesses get ahead of phishing and other cyber-threats. SC Magazine, 8 August https://www.scmagazineuk.com/breach-attack-simulation-bas-help-businesses-ahead-phishing-cyber-threats/article/1591352. Accessed 9 August 2019

McCue TJ (2019) From airports to the library: 5 steps to protect yourself on free public Wi-Fi. Forbes, 28 Jun https://www.forbes.com/sites/tjmccue/2019/06/28/from-airports-to-the-library-5-steps-to-protect-yourself-on-free-public-wifi/. Accessed 22 July 2019

Morgan L (2015) Polish airline forced to ground planes after "IT attack". IT Governance, 22 June https://www.itgovernance.eu/blog/en/polish-airline-forced-to-ground-planes-after-it-attack. Accessed 10 June 2019

Morris C (2019) Chinese hackers infiltrated eight major tech providers for years with 'devastating' impact: report. Fortune, 26 June https://fortune.com/2019/06/26/cloud-hopper-china-hacking/ accessed 15 July 2019

Masters G (2016) Ghost Squad hackers hit Trump sites with DDoS attacks. SC Magazine, 4 April https://www.scmagazine.com/home/security-news/ghost-squad-hackers-hit-trump-sites-with-ddos-attacks/. Accessed 30 July 2019

Olson P (2019) Marriott faces $124 million fine over Starwood data breach. The Wall Street Journal, 9 July https://www.wsj.com/articles/marriott-faces-123-million-fine-over-starwood-data-breach-11562682484. Accessed 19 July 2019

Palmer D (2017) Hackers are using hotel Wi-Fi to spy on guests, steal data. ZDNet https://www.zdnet.com/article/hackers-are-using-hotel-wi-fi-to-spy-on-guests-steal-data/. Accessed 20 July 2019

Park S-S and Lee H-S (2016) Asiana Airlines' customer database leaked on internet. The Korea Times, 18 July http://www.koreatimes.co.kr/www/news/biz/2016/07/123_209639.html. Accessed 22 July 2019

Perez R (2017) Travel trade body ABTA suffers data breach, 43,000 affected. SC Magazine https://www.scmagazineuk.com/travel-trade-body-abta-suffers-data-breach-43000-affected/article/1475030. Accessed 15 June 2019

Positive Technologies (2019) Vulnerabilities and threats in mobile applications 2019 https://www.ptsecurity.com/ww-en/analytics/mobile-application-security-threats-and-vulnerabilities-2019/. Accessed June 20 2019

Pulkkinen AJ, Vainio VV, Leino SP and Anttila JP (2018) Modelling of digital extended enterprise. In: International Dependency and Structure Modelling (DSM) Conference, Trieste, 15-17 October 2018, pp 139-152

PwC South Africa (2018) Hotels outlook report 2018-2022 https://www.pwc.co.za/en/assets/pdf/hotels-outlook-18-2022.pdf. Accessed 11 May 2019

Robinson T (2014) Shareholder sues Wyndham board members over data breaches. SC Magazine, 7 May https://www.scmagazine.com/home/security-news/shareholder-sues-wyndham-board-members-over-data-breaches/. Accessed 15 July 2019

Sabre (2017) Sabre update on cybersecurity incident https://www.prnewswire.com/news-releases/sabre-update-on-cybersecurity-incident-300483654.html. Accessed 12 July 2019

Schaal D (2019) Marriott CEO tells senators passport changes being considered after data breach, Skift, 7 March https://skift.com/2019/03/07/marriott-ceo-tells-senators-passport-changes-being-considered-after-data-breach/. Accessed 12 July 2019

Schwab K (2017) The fourth industrial revolution. Penguin Random House, London

Schwartz MJ (2018) British Airways faces class-action lawsuit over data breach. Bank InfoSecurity, 10 September https://www.bankinfosecurity.com/british-airways-faces-class-action-lawsuit-over-data-breach-a-11478. Accessed 12 July 2019

Seon (2018) We tried to buy travel tickets on the dark web: here's what we found https://seon.io/resources/2018/08/02/dark-web-travel-industry-fraud/. Accessed 22 July 2019

Sheridan (2018) For $14.71, you can buy a passport scan on the dark web. DarkReading, 4 October https://www.darkreading.com/vulnerabilities---threats/for-$1471-you-can-buy-a-passport-scan-on-the-dark-web/d/d-id/1332970. Accessed 28 May 2019

Sheridan (2019) Destructive malware attacks up 200% in 2019. DarkReading, 5 August https://www.darkreading.com/endpoint/destructive-malware-attacks-up-200--in-2019/d/d-id/1335444. Accessed 6 August 2019

Smith L and Read B (2017) APT28 targets hospitality sector, presents threat to travellers. FireEye https://www.fireeye.com/blog/threat-research/2017/08/apt28-targets-hospitality-sector.html. Accessed 22 May 2019

Statista (2019) Online travel booking worldwide https://www.statista.com/outlook/262/100/online-travel-booking/worldwide. Accessed 16 July 2019

Taylor I (2019) Online travel giants named in Facebook data-security breach. Travolution, 4 January https://www.travolution.com/articles/109903/online-travel-giants-named-in-facebook-data-security-breach. Accessed 30 July 2019

Trustwave (2016) New Carbanak/Anunak Attack Methodology , 14 November https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/new-carbanak-anunak-attack-methodology/ Accessed 22 July 2019

Trustwave (2019) 2019 Trustwave global security report https://www.trustwave.com/en-us/resources/library/documents/2019-trustwave-global-security-report/. Accessed 12 July 2019

Verizon (2018) Data breach investigations report 2018 https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf. Accessed 6 July 2019

Wall M (2018) Firms buy insurance 'in mad panic' as cyber-attacks soar. BBC News, 16 January https://www.bbc.co.uk/news/business-42687937. Accessed 23 May 2019

Whitehead J (2018) Booking.com targeted by hackers with email scam asking customers for payment details. The Independent, 4 June https://www.independent.co.uk/travel/news-and-advice/travel-website-hackers-cyber-crime-phishing-holidays-a8382771.html. Accessed 23 May 2019

Wilczek M (2019) The DDoS landscape: where we are, and where we're going. Information Age, 14 January https://www.information-age.com/the-ddos-landscape-123478142/. Accessed 23 July 2019

Winder D (2019) Security systems of major hotel chains exposed by huge data breach. Forbes, 31 May https://www.forbes.com/sites/daveywinder/2019/05/31/security-systems-of-major-hotel-chains-exposed-by-huge-data-breach/. Accessed 12 July 2019

World Economic Forum (2018) Regional Risks for Doing Business 2018. http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf. Accessed 16 July 2019

Wueest C (2019) Two in three hotel websites leak guest booking details and allow access to personal data. Symantec, 9 April https://www.symantec.com/blogs/threat-intelligence/hotel-websites-leak-guest-data. Accessed 15 May 2019