International Journal of Recent Advances in Multidisciplinary Topics
Volume 2, Issue 11, November 2021
https://www.ijramt.com | ISSN (Online): 2582-7839

Effect of e-Crime (Cybercrime) on Indian Tourism Industry

Sadhana Gautam[1*], Madhav Tyagi[2], Mahima Tyagi[3], Shubham Gautam[4], M. K. Gupta[5]
[1]*Research Scholar, Department of Commerce, Barkatullah University, Bhopal, India*
[2, 3, 4] *Research Scholar, Department of Commerce, Barkatullah University, Bhopal, India*
[5]*Head of the Department, Department of Commerce, Dr. Shyama Prasad Mukharjee College, Barkatullah University, Bhopal, India*

***Abstract*: As the tourism and travel sector is implementing evolving technologies to redefine services, products, and consumer experiences, their cyber ecosystems become increasingly vulnerable to security risks associated with these technologies, the vast number of economical transactions they carry out and the valued customer information they store. Over the past few years, numerous high-profile organizations in the sector made negative headings because they did not pay suitable attention to these risks and acquired a method to cyber security that was fragmented, technology-focused and compliance-oriented. It is obvious that a step change is required, and this chapter presents a more complete, business-driven and risk-based method to building cyber security capability in an organization. The chapter begins with the business case for a cyber-security policy and then clarifies the workings of a risk-based approach to cyber security.**

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

1. Introduction

It is a crime that includes the computer and network or the crime that contains a target or network. In this a computer has been used for causing harm individually or personally cyber-crime may harm someone security and financial help when a confidential information is disclosed it can cause a distress for both governmental and non- governmental including espionage, financial theft and other type of cyber -crime. When cyber-crime crosses the international border and including the other nation, referred as cyber warfare. WARREN BUFFET describes the cyber-crime as the "number one problem with mankind and poses real risks to humanity". In modern era the uses of cyber is increasing day by day we can't imagine our life without computers and technology. The use of technology is making the things easier for us but the use of computer is not safe because of cyber-crime its already a big problem all over the world growing so fast, in other words we can say the cyber-crime is illegal internet mediated activity that frequently take place in worldwide electronic media. Cyber-crime is "International" or "Transitional" there are no cyber borders between countries. International cyber- crime frequently increases the efficacy of local and international law and law enforcement sins subsist laws in many countries are not customized deal with cyber-crime, offenders progressively conduct the internet crimes for taking the advantages of the less severe punishments or struggling of being traced. Numerous organizations and governments have previously corporates and do efforts in demonstrating the worldwide standard of legislation and law enforcement on both regional and international scale. US and CHINAS cooperation is one of the noticeable progresses recently because they are the two top source countries of cyber-crime.

Cyber-crime is defined as the "offences that are committed against individuals or group of individuals with a criminal motive to harm intentionally harm the victim's reputations or cause the mental, physical harm to the victim directly or indirectly using modern technology networks such as internet (chatroom, emails) and mobile phone (SMS/mms)".

As the world is becoming smaller, cyber is getting bigger and moving into many new directions serving to fuel an unparalleled growth in consumer and business companions' expectations. It is growing beyond the organization's four walls and IT environments and moves into the products and amenities they provide as well as into the partner, seller, customer and stakeholder networks they produce. However, this digital change in tourism and travel which includes online transactions, cloud integration, customer analytics, connected devices, and digital payment technology also focusses to the realisation that, by increasing their digital footprint, organizations are progressively exposed to cyber threats.

Cyberattacks can be significantly unfavourable to customer trust and brand status and frequently have severe financial, legal and regulatory consequences. Kaspersky Lab (2018) estimates that it costs more than Rs 50,00,000 to recover from a security breach. These are only direct losses: money businesses are enforced to spend on IT recovery facilities, to cover lost business and interruption as well as legal and public relations facilities. Indirect losses i.e., costs for extra staff training and hiring, infrastructure advancements etc. are estimated, on

*Corresponding author: Sadhana.gm11@gmail.com

average, Rs 7,00,000. Then there are penalties to be paid. Three data breaches in Wyndham Hotels and Resorts' computer network between 2008 and 2010 negotiated records of over 600,000 guests with Rs 1 crore of fake credit card charges.

2. Wi-Fi Network / Website Compromise

Threat actors also take benefit of unsecured public networks in cafés, hotels, airports and tourist attractions to intrude traveller gadgets, and infect them with malware and also steal their personal data or use them as unintentional insiders for other targets. Apart from these attacks by means of Wi-Fi vulnerabilities like the Dark Hotel group explained previously, threat actors also use a technique known as the 'evil twin' attack. They locate themselves close to an authentic Wi-Fi access point (e.g., a museum's public Wi-Fi network) and discover its service set identifier (SSID) and frequency. Then they send a radio signal using the particular same frequency and SSID which to the other museum travellers appear as the authentic hotspot with the similar name. When visitors link to the evil twin, threat actors take control of their gadgets, gather their personal information and can monitor every action performed in the device. Evil twins are previously identified as honeypots or base station clones and are one of the greatest common cyber threats in the travel and tourism sector (McCue 2019).

Tourism and travel organizations' sites are additional attack vector for stealing valuable customer information, including Personal Identifiable Information and payment details. Research (Greif 2018; Wueest 2019) has revealed that major airline and hotel websites leak comprehensive guest booking data (including full name, address, mobile phone number, booking reference code, passport number, and the last four digits of credit card numbers) to third-party advertisers, social media websites, data collectors, and other partners. Some websites leak guest data to online associates during the booking process itself, while others leaked it when clients logged in to their booking page. Threat actors can access and use this data to log into a booking, view personal details, and even modify or cancel the booking.

1) The cyber security scenario in the present tourism industry

Observing at the past cases of cybersecurity problems and data breaches, it can be understood that tourism companies are hardly serious about cyber security till the bitter instant of truth really hits them. Though, there has been a change in the perspective of late.

But why are attackers aiming businesses in the travel and tourism industry? Tour companies, hospitality groups, airlines and car rental service agencies have a huge amount of customer data which can be pretty useful for cybercriminals in the long run. And then they try to detect vulnerabilities and openings in the systems of travel organizations. And meanwhile most travel companies depends on online platforms and reservation portals for business growth, this makes the private information susceptible to breaches on networks with low security protocols and guidelines in place. In fact, the whole network of dependency on third-party vendors makes it easier for the attackers to get hold of sensitive information.

2) Fundamental cyber security tips for the future of travel companies

Therefore, it is high time that tourism companies get thoughtful about cyber security because of the nature of data kept by them. While some simple tips can be taken at the start, a full-proof plan must be evolved to totally eliminate the odds of data breaches internally or through third-party servers. Here are a few tips that can help corporations' firm up their cyber security systems:

1. They must confirm monitoring of incoming and outgoing message for data-lifting malware.
2. A protected CRM system with user consents to lessen chances of data misuse must be put in place.
3. Uninterrupted use of unsafe websites on company servers needs to be blocked.
4. There must be control over the availability to backend data servers and systems.
5. Using updated anti-malware products and anti-virus software is a fundamental requirement.
6. Strong passwords for data safety must be employed.
7. Workers must be prohibited or barred from opening an email attachment from unidentified sources.
8. The corporations must put in place tokenization and data encryption procedures to protect sensitive data.

By using these simple tactics, even a small or mid-scale firm can advance its cyber security awareness. And as soon as the basic measures are in place, it is always a better thing to conduct a cyber-security audit and take an expert on-board to make the systems entirely immune to cyber-attacks.

3. Conclusion

The future tourism and travel cyber-ecosystem will progressively adopt new and disruptive technologies to deliver anytime and anyplace access. It will use virtualization, automation, software-defined networks and hybrid data centres and organizations in the area will be essential by their markets to architect additional flexible operationally secure environments. Several high-profile organizations in the sector made the headlines over the previous years because they did not pay this another requirement the attention that was required. Although certainly, the awareness of cyber threats among organizations in the sector is growing rapidly, threat actors are discovering new and creative ways to reach their objectives. For example, they use authentic questionnaire-hosting and file-sharing services from trusted corporations to avoid the blocking of their phishing attacks or using genuine restaurant websites as 'watering holes' to plant malware to organizations' networks when their staffs browse the menu from their secured devices. As the threat vector continues to grow, traditional cybersecurity strategies and tools are slowly becoming ineffective. People, processes, and technology have no choice but to develop so that they can support the new improved security needs.

References

[1] Biesiada J (2017) How to not fall victim to fraud. Travel Weekly, 22 September
[2] https://www.travelweekly.com/Travel-News/Travel-Agent-Issues/Insights/Ways-to-not-fall-victim-to-fraud
[3] Gallagher S (2016) Checking in with spear phishing, criminals check out with hotel credit card data. Ars Technica,
[4] Greif B (2018) Lufthansa data leak: what a single URL can reveal about you. CliqZ Magazine, 29 August
[5] Hill M (2018) Danish railway company DSB suffers DDoS attack. InfoSecurity Magazine, 14 May
[6] IBM (2018) 2018 IBM X-Force Threat Intelligence Index
[7] Kaushik S (2019) Cyberspace danger: can we really prevent internet fraud? Financial Express, 29 April
[8] Kumar A (2019) F-Secure talks up threat-hunting to stay ahead of cyberattacks in APAC. Computer Weekly, 25 July.