Middle East Research Journal of Economics and Management
ISSN 2789-7745 (Print) & ISSN 2958-2067 (Online)
Frequency: Bi-Monthly
DOI: https://doi.org/10.36348/merjem.2025.v05i03.002

KUWAIT SCHOLARS PUBLISHER
Website: http://www.kspublisher.com/
Email: office@kspublisher.com

Security Challenges & Techniques to Prevent Cyber Crime Threats in Tourism Industry

Dr. Gurjeet Singh[1*], Ms. Rupali Chopra[2]
[1]Vice Principal cum Professor, CKD Institute of Management & Technology Amritsar
[2]AP, Dept. of Tourism & Travel Management, CKD Institute of Management & Technology Amritsar

Abstract: Cyber security has a special role in protecting data across all industries. It is now more difficult to protect data from hackers. The tourism industry faces numerous cyber security challenges due to its reliance on digital technologies and handling of sensitive customer data. Multiple weaknesses are presented by the sector's intricate ecosystem, which includes several shareholders and massive volumes of confidential client data. Travellers and tourism companies are at serious danger from cyber threats like ransomware attacks, online fraud, data leaks and cyber-attacks on reservation systems. These risks may lead to economic damage, harm to one's reputation credibility, violation with standards, and diminished customer faith. To reduce these risks, tourism enterprises must emphasize effective cyber security measures. This includes installing network security systems, data protection, and security monitoring systems to protect private data and prevent illegal access. Employee training and awareness programs are also essential in identifying and preventing cyber threats. Regular security audits and vulnerability assessments can help recognize flaws and ensure compliance with industry standards. In addition, industry cooperation and data sharing are crucial for thwarting and combating cyber threats. Businesses in the tourism industry can improve their digital security posture by sharing threat intelligence, proven techniques, and knowledge gained. Tourism organizations can preserve trust, protect consumer data, and guarantee a safe travel experience by putting cyber security first and taking a proactive approach.

Keywords: Cyber Security, Information Security, Cyber Threats, Cyber Crimes Prevention, Regulations, Integrity.

Review Paper

***Corresponding Author:**
Dr. Gurjeet Singh
Vice Principal cum Professor, CKD Institute of Management & Technology Amritsar

How to cite this paper:
Gurjeet Singh & Rupali Chopra (2025). Security Challenges & Techniques to Prevent Cyber Crime Threats in Tourism Industry. *Middle East Res J Econ Management, 5*(3): 35-40.

Article History:
| Submit: 18.04.2025 |
| Accepted: 19.05.2025 |
| Published: 24.05.2025 |

1. INTRODUCTION

The biggest challenge nowadays is keeping sensitive data secure. To protect data from cyber attacks, all internet connected devices must have their security updated and upgraded. In addition to ordinary gadgets like PCs, smart phones and other internet connected devices; the cyber security department also handles technologies like servers, virtual machines, network topology, cloud services and more. IT organizations are required to evaluate and investigate cyber attacks since digital forensics is a component of this. Even while information security analysts and teams like SIEM and CISSP work for the companies to deliver quality work, attackers are developing new patterns to affect the CIA traid.

2. LITERATURE REVIEW

In the modern world, digitization and the internet have altered people's lifestyles by expanding social networks and business prospects. Cybercriminals on the other hand are using this platform to their advantage and breaking into networks to obtain private data. Cyber security professionals in the IT industry can guard against this risk of exploitation. The ARPANET research project in the 1970s gave rise to the term "cyber security". The researcher Bob created a tool that he began referring to as CREEPER when he used it to observe detectable footprints along the network path. Later, the same program was modified with the capacity to replicate itself by Ray Tomlinson, the man who created the email service. He created a program named REAPER to defend his invention of the first computer worm. Numerous cyber security strategies have been created recently to combat both domestic and foreign cybercrimes. The likelihood of being a victim is high because this digital ecosystem is merely a triangle made up of people, processes, and technology. In order to preserve security funds have been raised competitively by small businesses with 50% in 2018 and 66% in 2019,

as well as by large company sectors with 63% in 2018 and 67% in 2019. The primary goals of cyber security which are also seen as significant problems in both private and business life are to protect against cyber attacks, identify risks quickly, recover data loss and stop systems from becoming more vulnerable.

3. Importance

The importance of the Internet in modern life allows hackers to take advantage of greater opportunities. Thus, keeping the internet fast is just as crucial as keeping it secure. The majority of corporate transactions, private information, personal interests, and emotions are processed online. In addition to the IT industry, cyber security is one of the rapidly expanding professions in the public, government, healthcare, banking, education, and military sectors. Even national governments are enacting new cyber security rules and regulations to safeguard the availability, confidentiality, and integrity of data and services. Cyber security is important for protecting company data in every industry. To stop unintentional insider attacks, staff must be properly trained and adhere to security standards. Hiring cyber analysts for the organization's security can aid in the incident response process as well as threat identification. System security experts are crucial for looking into the issue and putting safeguards in place to stop attacks.

4. Hypothesis Testing

Cyber security offers numerous potential advantages that contribute to a company's expansion, reputation, and confidence in the community. By putting firewalls or access control lists in place, systems can be protected from exploitation of vulnerabilities and malware like as viruses, trojans, worms, and other spam or junk files. As a result, systems are secured from many hacking methods, including ransomware and denial-of-service attacks. Data loss and sensitive information exposure can be avoided with the use of security techniques. It is possible to reduce system or server crashes and preserve availability. There are many benefits to this, but there are also some drawbacks that should be taken into account. A single point of failure makes it simple to undermine centralized designs used for system security, such as unified threat management systems. A single point of failure could lead to failure, as the saying goes, "don't put all your eggs in one basket." The cost of hiring security professionals and creating security architectures depends on the size of the network. Intentional insider attacks may result from providing employees with adequate cyber security training. Even firewalls, when configured incorrectly, can occasionally fail to detect malicious file patterns. Cybercrimes for financial gain are more common in the cases of small start-up businesses and private citizens. As the business expands, more data and resources are available, which raises the complexity of the network. This makes network separation and security implementation difficult. Another issue to think about is developing security matrices that are scalable and adhering to security principles without exceptions.

5. Cyber Crimes

Cybercrime is defined as any unlawful behaviour carried out using a computer or the internet. The concept has been expanded to include identity theft, bullying, network penetration, and the spread of malicious files into systems. Since the majority of sensitive information is always stored in digital format, data security and privacy will be the top priorities for every business or organization. Emotional cheating and scams might eventually result from using hacking techniques like eve dropping or social engineering to access daily communications through social websites as well as company information. The most common type of cyber fraud is obtaining personal information for financial benefit. Malaysia had an increase of 82.5% in cyber security instances, according to the Cyber999 report. There will be a significant amount of assaults against Android phones in addition to computer or server threats. Accessing any week-secured device can result in whole network vulnerability because smart phones and other IoT devices are connected to other IoT devices already in place. Businesses and consumers have no choice but to accept the computerized world as technology and the internet continue to persuade people with their quick and easy ways of handling tasks. In 2015, there were 66% more cyberattacks than in 2009, according to the PwC security report. Confidentiality is being jeopardized, and the risk of sensitive information is growing quickly. Taking the 2017 Wanna Cry ransomware assault as an example, it is the most well-known cyber attack to have occurred in the United Kingdom. Around 200,000 computers worldwide, in 150 countries, were infected by the Wannacry outbreak, which began on May 12, 2017, and cost £6 billion. When the attacker's malicious email is opened, it starts downloading and running automatically on the computer. This secures the machine and its private information. The attacker then demands cryptocurrency as ransom. About 19,000 doctor's appointments, surgeries, and emergency patient treatments were cancelled as a result of the UK's national health service requesting £230 to unlock the computer.

6. Cyber Security

As technology is developing so quickly, cyber dangers have no boundaries and there is no room for slowing down. Threat actors committing cybercrimes such insider threats, storage device theft, and social engineering continue to harm businesses even when security regulations and policies are followed. Cyber dangers have spread beyond businesses and people's lives to include power plants and other utility services, leading to international cyberwar. Globally, cybercriminals are now concentrating on financial gains. Attacks using the Wanna Cry and Not Petya ransomware are good illustrations of worldwide cyber threats. Bit currency mining and individual bank account skimming

are two current strategies that have led to significant financial fraud. This has an effect on both monetary loss and public confidence in the government and banking industries. Businesses in the IT sector are less concerned with security and more with financial and international expansion. Offering a cutting-edge technological system for the organization's security is just as crucial as putting it into practice with the right setups for a safe environment. Establishing one's own security procedures to protect data and recognizing and thwarting threats early on are smart approaches to secure a business. Cyber experts can accomplish malware, which includes computer viruses, worms, trojans, adware, spam, ransomware and more is the most frequent danger to computers and networks in every industry. These are designed to inadvertently or purposely damage computers. Adopting technologies like machine learning approaches to secure websites and spam filters like intrusion detection and intrusion prevention systems are helpful for recognizing and blocking questionable files because malware programs can be created with various patterns to get past firewalls. Confidentiality and integrity cannot be compromised as long as the organization's business model is integrated into the security design and operations. The PPT framework is essential for managing structure and upholding standards in an organization. This framework, which is also useful for incident response, is the arrangement of people, processes, and technology. Using a DDOS assault on the company's server as an example service unavailability results. There are three components to the action: the criminal, the method he employed, and the tools he used. The framework is also known as the "three pillars of cyber security" because of its three constituents.

7. Cyber Security Implementation

Buying smart high tech gadgets to secure the system or an organization is successful only when the technology is implemented properly with required configurations. Such of the most popular technologies reflecting impact on cyber security are presented below:

7.1 Web Servers

Since the internet handles the majority of daily tasks, businesses have begun creating web-based applications to make life easier. The number of online attacks aimed at exposing or stealing private information is likewise rising. Via inadequately secured web servers, cybercriminals are leveraging the internet as an open platform to disseminate harmful files. Thus, web security and application security became a big worry. Cyber attacks can be avoided by using browsers with built-in virtual private networks.

7.2 Mobile Networks

Despite the widespread use of laptops and desktop computers, mobile technology is taking over the internet. With the exception of businesses or organizations where security is a problem, individuals are more accustomed to utilizing smart phones and tablets. The majority of daily private items in an individual's life are recorded on their own mobile phones. As a result, disregarding security updates results in more pay. In order to combat network intrusion assaults, security and network speed have been improving as mobile networks have transitioned from 4G to 5G.

7.3 Changing to IP6 Version

The backbone of the internet is Internet Protocol version 4, or IPV4, which connects a vast number of devices. As IPV4 is being replaced by IPV6, which allows more connected devices and has greater security features, the trend is now being reversed. By putting IPV6 technology into practice, assaults can be decreased in both private and large-scale IT sectors.

7.4 Cloud Based Services

Targeted database assaults are becoming more common in the public and military sectors in addition to the IT and healthcare industries. Cloud storage proved to be the best way to address the issue and stop SQL injection attacks. As a result, cloud services are being adopted by the majority of industries, both large and small. Cloud storage capacity varies as information volume increases, leading to security vulnerabilities. Software as a service, platform as a service, and infrastructure as a service are other examples of services. Additionally, this aids users in resource conservation and security.

7.5 Data Encryption

The process of transforming a human-readable format into a coding format is called encryption. The method is employed to stop attacks such as man-in-the-middle and eavesdropping. A key that specifies the type of encryption is used to convert data using a few technical encryption methods. Although this method is not new, the strength of the encryption depends on the number of bites. Salting is an encryption technique that makes encryption difficult to penetrate. Despite being exposed, this preserves the confidentiality of the data.

7.6 Suitable Technology

The suitable technologies used to maintain security system stronger are as follows:

- **Firewall:** The first line of defence for a system or organization is a firewall, which can be either hardware or software. A firewall's job is to filter and inspect packets, but it's important to set it up correctly because a firewall with the wrong configuration can be circumvented by altering the file pattern.
- **Anti-Virus Applications:** Malware can slow down a system, cause crashes, erase or replace files and even assist an attacker in compromising a system or servers. These consist of ransomware, spyware, worms, trojans, viruses and more. Malware scanners also referred to as anti-virus software, can identify certain types of malicious software. Anti-virus

software's job is to search the entire system for suspicious files and then identify, block, or remove them. However, there are a few drawbacks, such as increased RAM usage, sharing of private data, and lack of support for full protection.

- **Honey Pots:** Honey pots are a type of security alarm that has been developed in recent years to assist administrators or security analysts in locating intruders. These are employed to divert the hacker's attention and stop the data from being stolen. Although the initial step of an assault can be avoided with this technology, incorrect setups may result in false alerts.
- **User Credentials:** Entering user credentials is the initial stage in the authentication and authorization process for computer or web application access. Entering a username and password, which determines each user's uniqueness, is the standard method of access because the hacker can use these to impersonate the user. We refer to this as a social engineering attack. The most recent remedy to this issue is a one-time password (OTP). This is a special password that is provided to the email or mobile device. Another name for this is three-way authentication.
- **Access Control Lists:** As cyber risks increase, maintaining an access control list (ACL) to allow access to files based on their sensitivity is becoming more popular. ACL is used to block a particular set of users or to generate a specified list of people who have the ability to access files or directories. Organizations primarily employ this to protect extremely sensitive data from insiders. Typically, the list is based on the employee's function and criteria.

7.7 Cyber Risks in Tourism Industry

Cyber risks are any events that involve unauthorized access, use, or damage of electronic data or systems. Some common examples of cyber risks are:

- **Phishing**: This is when hackers send fraudulent emails or messages that look like they come from legitimate sources, such as banks, suppliers, or customers. They try to trick you into clicking on malicious links or attachments, or providing sensitive information, such as passwords or credit card numbers.
- **Malware**: This is any software that is designed to harm or disrupt your computer or network. It can include viruses, worms, trojans, ransomware, spyware, adware, etc. Malware can infect your devices through phishing emails, malicious websites, removable media, or software downloads.
- **Ransomware**: This is a type of malware that encrypts your data or locks your system and demands a ransom for restoring access. Hackers can threaten to delete your data, expose it publicly, or sell it to other criminals if you don’t pay the ransom.
- **Data Breach**: This is when hackers gain unauthorized access to your data and steal it, modify it, or delete it. They can use your data for identity theft, fraud, blackmail, or other malicious purposes. They can also sell your data to other hackers or competitors.
- **Denial-of-Service (DoS) Attack**: This is when hackers overwhelm your website or network with a large amount of traffic or requests, making it slow down or crash. This can prevent you from providing services to your customers, resulting in lost revenue and reputation.

7.8 Cyber risks for the Tourism Industry

- Tourism businesses collect and store a lot of sensitive data from their customers, such as names, addresses, IDs, passports, credit cards, travel plans, preferences, etc. This data is valuable for hackers and can cause serious harm to your customers if compromised.
- Tourism businesses rely heavily on online platforms and systems for booking, payment, communication, marketing, etc. These platforms and systems can be vulnerable to cyber-attacks and cause operational disruptions and financial losses if compromised.
- Tourism businesses operate in a highly competitive and dynamic market. They need to maintain a high level of customer satisfaction and loyalty. A cyber incident can damage their reputation and trustworthiness and cause them to lose customers and market share.

7.9 Prevent and Mitigate Cyber Risks

The best way to protect your tourism business from cyber risks is to adopt a comprehensive and proactive approach that includes:

- **Employee Training**: Your employees are the first line of defence against cyber risks. You need to train them on how to identify and avoid phishing emails and other suspicious messages. You also need to educate them on the importance of using strong passwords and multifactor authentication for accessing your systems and data. You should also have clear policies and procedures for reporting and responding to any suspicious or malicious activity.
- **Endpoint Protection**: Your devices (such as computers, laptops, tablets, smart phones) are the entry points for hackers to access your network and data. You need to use reputable antivirus software on your devices and keep them updated with the latest security patches. You also need to use encryption to protect your data in transit and at rest.
- **Network Security**: Your network (such as routers, switches, firewalls) is the backbone of your online operations. You need to secure your network from unauthorized access and intrusion by using firewalls, VPNs (virtual private networks), SSL (secure sockets layer) certificates, etc. You also need to monitor your network traffic and activity for any anomalies or signs of attack.

- **Cloud Security**: Your cloud services (such as email hosting, web hosting, data storage) are the lifeline of your online presence. You need to choose reliable and reputable cloud providers that offer high levels of security and privacy for your data and systems. You also need to review their terms and conditions carefully and understand their roles and responsibilities in case of a cyber incident.
- **Risk Assessment**: You need to conduct regular risk assessments to identify and evaluate the potential cyber threats and vulnerabilities facing your business. You need to prioritize the most critical assets and processes that need protection and implement appropriate controls and measures to reduce the risk exposure.
- **Risk Mitigation Solution**: You need to use a risk mitigation solution that will help you monitor and manage your off-premise risk profile: any leaked information or exposure across the web. This solution will alert you of any potential breaches or incidents involving your business and help you take corrective actions.

7.10 Cyber Incident

Despite your best efforts, you may still face a cyber incident that can cause significant damage and losses to your business. This is where insurance can help you. Insurance can provide you with a defined incident response process and access to leading experts who will help you with your breach. These experts include:

- **An IT Forensic Team**: They will come in when you realize that you have a breach and help you get back up and running as soon as possible. They will investigate the cause and extent of the breach, contain and eliminate the threat, recover and restore your data and systems, and prevent future attacks.
- **Legal Experts**: They will assist you with liability issues. They will advise you on your legal obligations and rights, such as notifying your customers, regulators, or law enforcement authorities. They will also help you defend yourself against any lawsuits or claims from third parties.
- **A Reputation Management Team**: They will assist you with brand reputation damage. They will help you communicate effectively with your stakeholders, such as customers, employees, partners, media, etc. They will also help you rebuild your trust and credibility in the market.

➢ **Your insurance policy will also cover various costs and expenses that may arise from a cyber incident, such as:**

- **Ransom Payment**: If you are a victim of ransomware, your policy will cover the ransom payment to the hackers. The experts will negotiate with the hackers to lower the ransom amount and verify that they have the decryption keys. They will also try to decrypt your systems without paying the ransom if possible.
- **Business Interruption**: If your business operations are disrupted or suspended due to a cyber incident, your policy will cover the loss of income and the extra expenses that you incur to resume your normal operations.
- **Data Restoration**: If your data is corrupted or deleted due to a cyber incident, your policy will cover the cost of restoring or recreating your data from backups or other sources.
- **Liability and Compensation**: If your customers or other third parties suffer any harm or loss due to a cyber incident involving your business, such as identity theft, fraud, or breach of contract, your policy will cover the legal fees and the settlement amounts that you have to pay.

7.11 Insurance for your Tourism Business

Cyber insurance is not a one-size-fits-all solution. You need to choose the right insurance for your tourism business that suits your specific needs and budget.

Some factors that you need to consider when choosing cyber insurance is:

- **The Scope of Coverage**: You need to check what types of cyber risks and incidents are covered by the policy and what are excluded. You also need to check what types of costs and expenses are covered by the policy and what are not.
- **The Limit of Liability**: You need to check how much the policy will pay for each claim and for each policy period. You also need to check if there is any deductible or co-payment that you have to pay before the policy pays.
- **The Premium Rate**: You need to check how much the policy will cost you based on various factors, such as your industry, size, revenue, risk profile, security posture, etc. You also need to check if there are any discounts or incentives that you can avail based on your security measures or practices.
- **The Claims Process**: You need to check how easy and fast it is to file a claim and get paid by the policy. You also need to check how responsive and supportive the insurer is in case of a cyber incident.

7.12 CONCLUSION

There are countless advantages to cyber security, but there are also very few drawbacks. The victims of these cyber attacks included even major security companies. Businesses that handle sensitive data and lack cyber security expertise, such as those in the banking and medical industries, are particularly vulnerable to cyber attacks. To combat cybercrimes, the company can benefit from hiring someone to handle cyber security operations. Among other things, businesses have a need to provide their staff with appropriate cyber security training. This aids staff members in spotting the attack early on, which may not help with attack defence but may help reduce the damage. Although this inadvertently teaches workers

how to carry out insider attacks covertly, this can be lessened by putting in place ongoing security and surveillance measures. The tourism industry must prioritize cyber security to protect customer data prevent financial losses and maintain a positive reputation. By deploying strong security protocols and tactics tourism enterprises can minimize the risk linked with cyber crime threats and ensure a safe and secure experience for travellers. Cyber protection solutions are very affordable and highly sophisticated. There are many tools and services available that can help you secure your data and systems, monitor your risk exposure, and respond to any breaches or incidents.

REFERENCES

- Anderson, C., & Wilson, D. (2023). "Cyber security in the Age of AI: Challenges and Opportunities." Journal of Artificial Intelligence and Cyber security, 5(2), 89-104.
- Bai, R., Chandra, V., Richardson, R. & Liu, P. P., (2020) “Next Generation Mobile Wireless Networks: 5G Cellular Infrastructure”, The Journal of Technology, Management, and Applied Engineering 36(3).
- Brown, R., & Garcia, M. (2023). "Best Practices in Cyber security: Lessons Learned from Real-World Incidents." Journal of Information Security Management, 10(4), 213-230.
- Clarke, R., & Knake, R. (2023). "Cyber War: The Next Threat to National Security and What to Do About It." HarperCollins.
- Cyber Crime Reporting Cell. (2024). Trends in cyber-crimes and arrests in India: A comprehensive analysis.
- Dr. K. Kiran Kumar, Sk. Mahaboob Basha, S. Nividitha, 2016, A Survey of Cyber Crimes, International Journal of Engineering Research & Technology (IJERT) ICACC – 2016 (Volume 4 – Issue 34).
- Elliott C (2019) Hackers are targeting airlines in record numbers. Here's what that means for you. Forbes, 25February *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.
- Greif B (2018) Lufthansa data leak what a single URL can reveal about you. CliqZ Magazine,29August *https://cliqz.com/en/magazine/lufthansa-data*-leak-what-a-single-url-can-reveal-about-you. Accessed 23 July 2019.
- Johnson, T. (2022). "Emerging Trends in Cyber Threats: A Review of Recent Developments." International Conference on Cybersecurity Proceedings, 45-56.
- M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, “Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study,” J. Inf. Secur. Appl., 2020.
- M. M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” Computers and Security. 2020.
- Prometteur Solutions. (2023). Cyber Attacks in India: A Comprehensive and In-Depth Analysis. Retrieved from https://www.prometteursolutions.com/blog/cyber-attacks-in
- SANS Institute. (2023) "SANS 2023 Cyber security Trends Report." Retrieved from https://www.sans.org/security-resources/posters/cybersecurity-trends-report-2023.
- Smith, J., & Jones, A. (2023). "Understanding the Threat Landscape: A Comprehensive Analysis of Cyber security Risks." Journal of Cyber security Research, 15(2), 112-128.