Cyber Awareness for Ethnotourists: Navigating Risks in Cultural Experiences

Bobir Odilov,[1,a)] Durbek Sayfullaev,[2,b)] Nodir Karimov,[3,c)] Valisher Abirov,[4,d)] Islomjon Rustamboev[5,e)] and Zilola Sattorova[6,f)]

[1,2,3,4,6]*Tashkent State University of Oriental Studies, Tashkent, Uzbekistan.*
[5]*Oriental University, Tashkent city, Yakkasaroy district, Uzbekistan.*

[a)] *Corresponding author: odilov_bobir@tsuos.uz,*
[b)] *durbek_sayfullayev@tsuos.uz,* [c)] *nodir-karimov@list.ru,* [d)] *valisher_abirov@tsuos.uz,*
[e)] *islomjon_rustamboev@mail.ru,* [f)] *Zilola2022@list.ru*

Abstract. The goal of ethnotourism, a developing trend in cultural tourism, is immersive experiences in local communities. On the other hand, specific cyberthreats that affect ethnotourists include cultural appropriation, online harassment, and data breaches. This study examines the need for cyber awareness among ethnotourists, identifies hazards, and offers safe online participation guidelines. Ethnotourism exposes travellers to cyberattacks even though it offers fascinating cultural experiences. As technology increasingly mediates these experiences, it is imperative to have a firm grasp of the risks associated with cyberspace. As part of security, people also need to be shielded against cyberthreats, like identity theft and online fraud. The travel and tourist industry's cyber ecosystems are growing more and more susceptible to security vulnerabilities as a result of developing technology, the volume of financial transactions they process, and the important client data they keep. Products, services, and customer experiences are being redefined by means of these technologies. The process entailed searching web log files and linking events to identify anomalous behaviour. Systems that rely on logging can be advantageous for security incident monitoring. A framework for predicting insider intimidation has been found, drawing on multiple techniques from computer science and psychology. The real-time scrutinising tool searches for irregularities in user technological characteristics to investigate suspected network activities.

Keywords. Cultural Experiences, Tourist Industry's, Network Activities.

INTRODUCTION

One of the best resources for busy people in the twenty-first century is spare energy, which is being taken up by the travel sector. Because of this, a tourist is extremely driven, daring, and genuinely wants to appreciate the location they are visiting, but they are also extremely perceptive, demanding, and critical [1]. Tourism is defined by the emergence of new travel motivations and the ongoing changes in visitor demand patterns [2-3]. Travellers now demand an experience that encompasses both excellent lodging and services; they are not satisfied with a single tourism offer or simply a nice place to stay. Other tourist destinations can be found in the vicinity of the urban centers [4]. The expansion of continental tourism would enhance the quality of the traveler experience overall, enable year-round traveler supply (minimising seasonal variations in traveler numbers), encourage greater use of available lodging options, and ultimately increase traveler consumption [5-7]. Continental tourism has a good effect on the rural community and the general quality of life for the people living in the region, in addition to its economic benefits. Continental tourism can play a major role in the expansion of the economy [8]. The paper offers the results of study on visitors' attitudes and overall satisfaction based on an example of the activities that tourists participate in during their visit (excursion) to neighbouring sites. As previously mentioned, excursionists (compared to transit and residential tourists) make the largest part of tourist visits to the continental destinations [9]. The Cyber Risk Landscape shown in fig. 1.

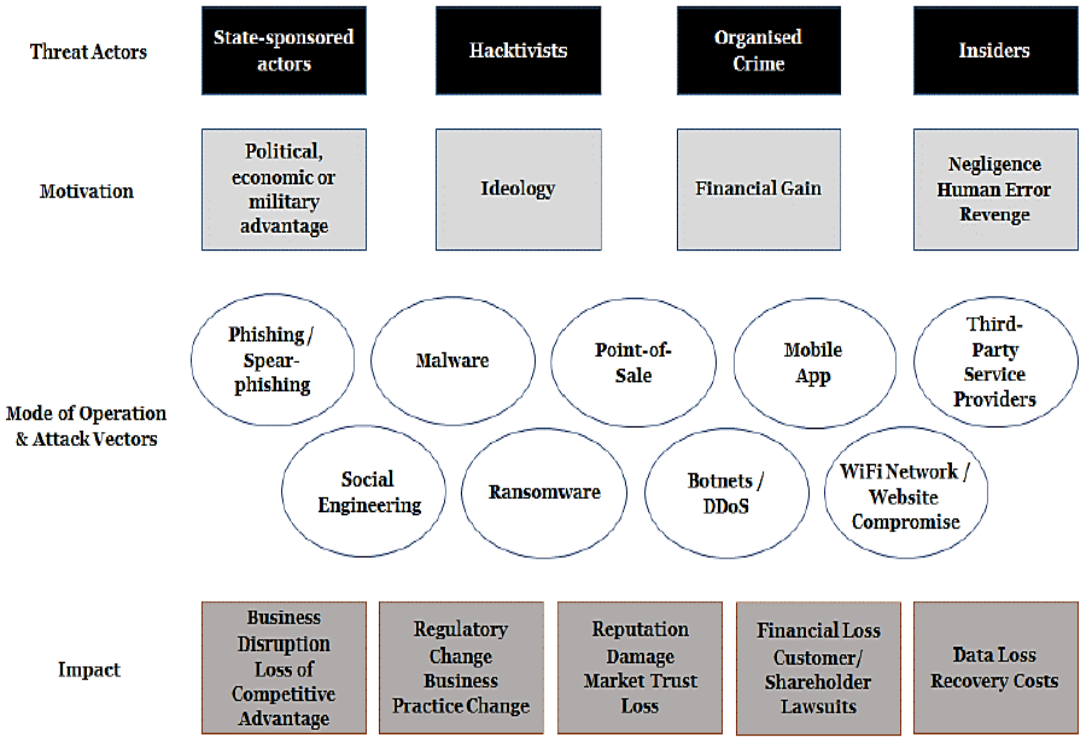

FIGURE 1. The Cyber Risk Landscape

A poll was conducted among excursionists, who account for a sizable fraction of travellers to continental destinations [10]. The study's findings demonstrate the significance of comprehending visitor behaviour and satisfaction levels while creating a tourism product. This explains why the study was conducted in Zagreb and the neighbouring areas, as people of Zagreb are probably going to travel to nearby continental destinations. The degree of demand from travellers for the Continental Croatia tourism offer will depend on how appealing and competitive the tourism offer is in this area. An integrated tourist offer allows for a more thorough examination of the special interest tourism categories that may serve as the foundation for this development. All destinations, particularly continental ones, must position their tourism development by keeping up with the latest trends and modifying their offerings to visitors. It cannot be overstated that each tourism destination should set its own trends by providing unique travel experiences that cater to the tastes of its target audience. Actually, because of the various changes that take place throughout time, there will always be a need to adjust some parts of the service.

LITERATURE REVIEW

Ethnic tourism is acknowledged as a tool for rural economic development according to Yang and Wall. It may offer chances for financial gain, diversify local livelihoods, and give local communities more economic clout. The bulk of research, however, has shown that top-down tourism development leads to an unequal distribution of benefits, with the economic and political elites capturing the majority of the benefits. This may not be the case in all places. Claims of broad economic empowerment and pro-poor advantages from tourism growth seem overstated according to Higgins-Desbiolles [9]. Before then, the main purpose of domestic tourism was to bring ethnic groups together with the Han majority for political purposes. Since the 1980s, several tiers of the Chinese government have embraced ethnic tourism as a means of stimulating the regional economy and reducing poverty [11]. Regarding the contribution that tourism makes to the development of rural and ethnic communities, they have always had favourable opinions [12]. Over the past few years, the growth of tourism in ethnic areas has helped many ethnic communities, especially in terms of better infrastructure and transportation. On the other hand, because tourism is a government-supported development tool, it is mainly driven by organisations outside of the ethnic villages that become tourist destinations [13]. The asserts that because ethnic groups have limited resources and expertise, the growth of tourism has a substantial effect on nearby communities [14]. The Chinese government at all levels views

economic gains as its primary goal and views ethnic culture as a resource that may be exploited. Top-down governance is common in many ethnic tourist locations, which limits the ability of ethnic minority groups to decide how their culture is portrayed in tourism products or promoted to the outside world. Cornet claims that when outside tourism developers are involved, money may be distributed unevenly, which could make host communities tense and resistive [15]. While community members do take part in decision-making in the village-based tourism that is so popular in rural China, there is also a great deal of disempowerment and disengagement of the community [16].

NAVIGATING RISKS IN CULTURAL EXPERIENCES

Additionally, an insider can use Bluetooth, WiFi, or flash drives with a smart device that has malware on it to connect to the organization's network. IoT risks are caused by threats that exploit weaknesses in IoT devices or the IoT environment. For example, information centres and nuclear power facilities could be hacked if IoT devices are employed to automate their operations. Cyber Attack shown in fig. 2.

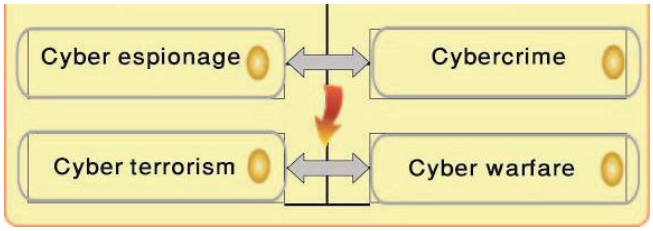

FIGURE 2. Cyber Attack

- **Ethical IoT Risk:** This is the term for the unanticipated negative consequences of unethical behaviour involving IoT devices. Volkswagen is a car manufacturer that created and set up software to rig diesel pollution tests. This action broke the Clean Air Act in the United States, jeopardised industry and organisational norms, and caused significant financial and reputational damages.
- **Privacy and Security IoT Risk:** This is the term used to describe the intentional harming of assets through the exploitation of system vulnerabilities. For instance, a DDoS attack against DYN in October 2016 by the Mirai (IoT specialised malware) Botnet caused outages on several websites, including Twitter, Netflix, CNN, Reddit, and many more. The temporary or permanent loss of control over data that is harmful to the organisation is referred to as the privacy IoT risk, and it falls under this category as well. eBay's May 2014 data breach resulted in the hacking of its customers' records, including passwords.
- **Technical IoT Risk:** This results from software or hardware malfunctions brought on by subpar development, testing, etc. It was recently discovered that semiconductors used in personal computers manufactured in the last 20 years have security weaknesses at the chip level. Meltdown, for instance, is a hardware vulnerability in Intel x86 microprocessors that allows a rogue function to access all memory even when it is not authorised to do so. Inadequate design compromises security and privacy. IoT hazards include the possibility of a phishing attack on a linked business device, such as a laptop or smartphone, infecting multiple IoT sensors with malware and disrupting a manufacturing plant's production line as a result.

Understanding the distinctive features of IoT systems and the causes of the shortcomings of the existing risk assessment methodologies for IoT is essential before delving into the analysis of IoT risk frameworks. Periodic assessments have limits in IoT systems because of the rapid and significant changes that can occur due to the interoperability of IoT devices. IoT solutions need to be evaluated on a regular basis. The Internet of Things (IoT) environment may provide new vulnerabilities and device breaches due to interconnected assets. Failure in IoT systems can also occur during the evaluation of the binding processes—that is, the connections that enable the devices to couple and function. In light of the aforementioned considerations, the conventional cyber risk assessment procedure needs to be modified for IoT systems. Internet of Things deployment differs from traditional IT because of its networking approach. The CIA trinity may not be supported by all of the networking models and devices used in the Internet of Things ecosystem. Technologies like data encryption, authentication, access controls, and automatic software patching or upgrades are examples of common precautions. IoT devices expand the attack surface despite being adaptable and interoperable. Applications, protocol upgrades, and device firmware updates all

contribute to an expanded attack surface that requires security. These factors should be taken into account while designing the IoT risk assessment methodology. The advantages and disadvantages of the majority of the commonly used IoT risk assessment frameworks are contrasted. The preceding section covered a number of CSRFs (Cyber Security Risk Frameworks), such as OCTAVE, NIST, ISO, etc. It goes without saying that because the concept of IoT introduces complicated hazards to assets and devices, more caution must be used while evaluating risk in the IoT context. As of right now, there are no established risk frameworks for IoT. However, there is room for small modification of the current risk assessment frameworks to address IoT concerns. All staff members are required to abide by a set of documented practices and processes known as security policies in order to guarantee the availability, confidentiality, and integrity of data and resources. With the aim of safeguarding the company, the security policy outlines the expectations for the enterprise, explains how they are to be met, and outlines the penalties for noncompliance.

CYBERSECURITY STRATEGY, MECHANISMS AND CONTROLS

The cyber-protection strategy should serve as the foundation for organisational policies and standards. It should address three key areas: risk management, consequence management, and the human element of the business. Critical System and Information Asset Risk Profiling shown in fig. 3.

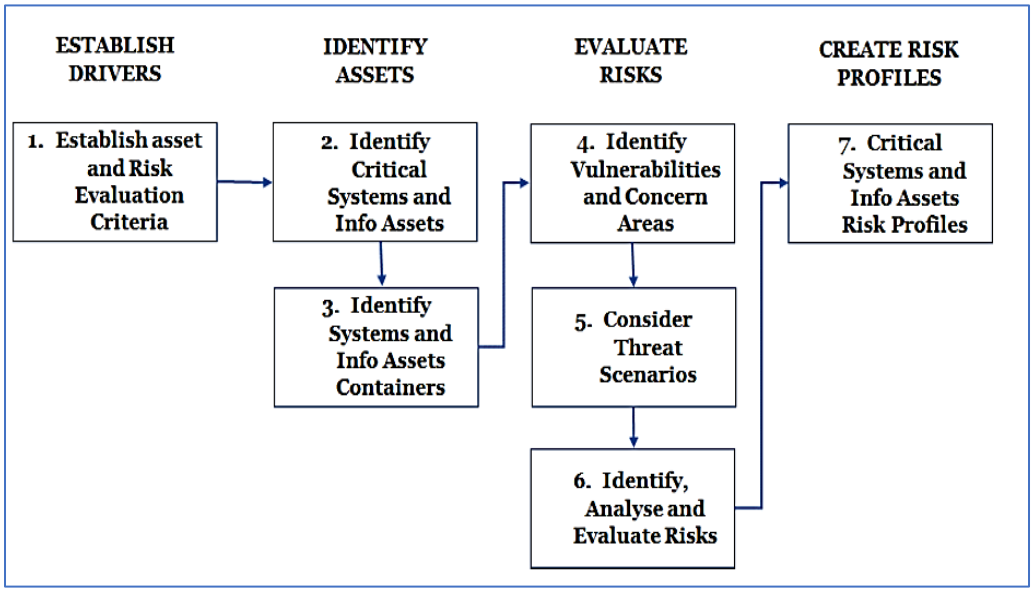

FIGURE 3. Critical System and Information Asset Risk Profiling

Since the majority of system failures and data breaches are caused by unintentional and malevolent insiders (workers, business partners, and third-party vendors), cybersecurity is more than just technical safeguards. The gap between human factors and strong cybersecurity practice often stems from how well-run communications and training programs engage staff and promote awareness. Programs that are appropriate for specific audiences, specific to the organisation, and in line with its operational objectives are necessary because, in most cases, they don't work for everyone. In addition to focussing on the unique threats, challenges, and responsibilities of each position, training must be customised to each trainee's privilege rights, physical and network access levels, and job responsibilities (for example, the curriculum for reservation agents will differ from that of finance staff and third-party vendors).

Reducing the vulnerabilities in an organization's digital ecosystem by strengthening defences and taking proactive steps to stop threat actors from targeting it is the second part of a cybersecurity strategy. It is necessary to decide on and create comprehensive standard operating procedures for important "cyber hygiene" issues such as system physical security, identity and access management, network segmentation, third-party and external dependencies, malware and patch management, information protection, and encryption. Travel and tourist

organisations continue to face basic cyber hygiene challenges, such as access management, despite this seeming paradox.

The third element of a cybersecurity plan is the organization's response in the event of an attack or data breach. A three-pronged crisis management plan comprising incident response, business continuity, and crisis communications must be developed by the organisation in order to manage and coordinate IT, operational, and systems recovery concerns associated to a cyberattack. A multifunctional crisis management team oversees all three plan components; contingent on the incident's severity, this team may include members of the C-suite. Nevertheless, specialised teams should normally be allocated to each of these facets.

FUTURE CYBERSECURITY DEVELOPMENTS IN TRAVEL AND TOURISM

The travel and tourism cyber-ecosystem of the future will increasingly employ innovative and disruptive technology to provide access at any time and from any location. The adoption of automation, virtualisation, software-defined networks, and hybrid data centres is anticipated, and companies in the industry will face market pressure to provide more flexible and operationally secure systems. Numerous well-known businesses in the sector have made headlines lately as a result of their failure to pay adequate attention to this second criteria.

Threat actors are developing creative and innovative ways to achieve their objectives, even as the sector's organisations are more conscious of cyber dangers. They use reputable companies' legitimate file-sharing and questionnaire-hosting services to avoid having their phishing attacks blocked, or they use the websites of takeaway restaurants as "watering holes" to infect networks of businesses with malware when workers use secure devices to peruse the menu. The expanding threat landscape is gradually rendering traditional cybersecurity techniques and solutions inadequate. The new, stricter security requirements necessitate changes to people, processes, and technology. The cybersecurity strategies used by these companies need to change from reactive to proactive. Consequently, instead of finding malware and attackers 20 or 50 days after they were installed and after they had already caused damage, they will actively seek for them before their networks are activated. The new cybersecurity tactic, dubbed "threat hunting", is now simpler because to advanced AI and Endpoint Detection and Response (EDR) technology.

The plethora of security lapses and breaches that have been publicised in the media will make data privacy and security one of the industry's key differentiators. Companies who view this component as nothing more than a compliance exercise risk losing the trust of the market over time. But more and more, the client will be the focal point of identity and access control. Consequently, travel and tourism companies will inevitably search for solutions that offer them flexibility and embrace more as-a-service delivery models (like PAMaaS, IDaaS, and others) that offer single sign-on, password less authentication, and multi-factor biometric authentication that is user-friendly [13]. As more businesses in the industry shift their IT infrastructure and data centres to the cloud, a "multi-cloud approach" for distributed reservations, yield and revenue management, channel/distribution management, call centres, and content management is becoming more popular. This is because the cloud offers flexibility, resilience, and significant cost benefits. However, using numerous clouds raises the likelihood of fragmented visibility, complicates the application of cybersecurity policies consistently, and makes it more difficult to manage information assets and systems in a safe manner. Travel and tourism companies will confront two primary challenges when personally identifiable data crosses various cloud boundaries: first, maintaining PCI compliance; and second, creating an integrated threat prevention plan that includes automated threat detection and response.

CONCLUSION

Cyberspace awareness is essential for ethnotourists to stay safe and show respect for the cultures they visit. By being aware of these risks and adopting safe internet habits, ethnoturists can enrich their cultural experiences while keeping themselves and the communities they visit safe. For a deeper knowledge of cybercrime concerns, the viewpoints of all parties or bodies involved—perpetrators, law enforcement, and victims—are equally significant. Consequently, the ultimate objective of the researcher is for the study's conclusions to act as a roadmap for policymakers, the government, the Ministry of Tourism, the Tourism Authority, and other stakeholders in the tourism industry when it comes to formulating policies, talking about cybercrime, and developing approaches to address the problem. That is to say, all matters pertaining to cyber vulnerability, countermeasures, and real-world situations involving travellers will be covered. In order to help tourists defend themselves and minimise or prevent

victimisation, policymakers and authorities will have a baseline from which to adopt policies and measures. For example, managers and planners of the tourism industry will be able to come up with ways to reduce the amount of cybercrime that travellers encounter. Understanding the various types of cybercrime that visitors encounter and suggesting preventative actions will put DMOs in a better position to offer helpful security information to prospective inbound tourists as part of their destination marketing operations. Such an action could improve the destination's reputation and image while also boosting inbound tourism.

REFERENCES

1. S. Nyhlén, S. Skott, and K. Giritli Nygren, "Haunting the Margins: Excavating EU Migrants as the 'Social Ghosts' of Our Time," *Critical Criminology*, 1-18 (2024).
2. M. E. Ohsfeldt, "To Play with Spirits: Fluidity and Distinction in Role-Playing Game Shamans," Doctoral dissertation (2017).
3. M. Masthan, "Changed Piezoelectric Design Regarding High Electric Power Growing Employing MEMS," *Middle-East Journal of Scientific Research*, **20**(4), 451-455 (2014).
4. D. Justice, "The Festival of World Sacred Music: Creating a Destination for Tourism, Spirituality, and the Other," *In the Changing World Religion Map: Sacred Places, Identities, Practices and Politics*, pp. 2833-2849 (2015).
5. K. Rice, "Rights and Responsibilities in Rural South Africa: Gender, Personhood, and the Crisis of Meaning", Indiana University Press (2023).
6. A. Fradkin, "Single Reviews," *American Anthropologist*, **110**(1) (2008).
7. A. Surendar, V. Saravanakumar, S. Sindhu, and N. Arvinth, "A Bibliometric Study of Publication-Citations in a Range of Journal Articles," *Indian Journal of Information Sources and Services*, **14**(2), 97–103, (2024). https://doi.org/10.51983/ijiss-2024.14.2.14
8. T. B. Falkowski, and S. A. Diemont, "Cultural Ecosystem Services in Agroforests," *Agroforestry and Ecosystem Services*, 361-387 (2021).
9. B. A. Odilov, and A. Madraimov, "Utilizing Deep Learning and the Internet of Things to Monitor the Health of Aquatic Ecosystems to Conserve Biodiversity," *Natural and Engineering Sciences*, **9**(1), 72-83 (2024).
10. A. Parsons, "Purveying Provincial Attitudes: Tourism Workers and the Creation of Commodifiable Culture in Nova Scotia," (2018).
11. Surendran, D., Arulkumar, V., Aruna, M., Sangamithrai, K., & Thangadurai, N. Improving the quality of education through data analytics and big data contributions. *In AIP Conference Proceedings*, **(2742)**1, 2024.
12. Guruprakash K.S, Siva Karthik P,Ramachandran A,Gayathri K, "Crop pest identification using deep network based extracted features and MobileENet in smart agriculture", *Land Degradation and Development*, **(35)**11, 3642–3652, (2024).
13. Cherukuri, Bangar Raju, and V. Arulkumar. "Optimization of Data Structures and Trade-Offs with Concurrency Control in Multithread Software Structures Using Artificial Intelligence." *IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT)*. **(5)**1, 2024.
14. T.M. Nithya, P. Rajesh Kanna, S. Vanithamani, P. Santhi, "An Efficient PM - Multisampling Image Filtering with Enhanced CNN Architecture for Pneumonia Classfication", *Biomedical Signal Processing and Control*, **(86)**2, 1746-8094, (2023).
15. M. Pásková, N. Budinská, and J. Zelenka, "Astrotourism–Exceeding Limits of the Earth and Tourism Definitions?," *Sustainability*, **13**(1), 373 (2021). https://doi.org/10.3390/su13010373
16. M. Pásková, and J. Zelenka, "Case Studies of Social Responsibility in Tourism," *In Social Responsibility in Tourism: Applications, Best-Practices, and Case Studies*, 137-158 (2024).
17. D. Bobojonova, "Traditions and History of Librarianship in Central Asia," *Indian Journal of Information Sources and Services*, **14**(2), 70–77 (2024).
18. H. A. Friedl, "Western Money for Southern Sympathy: How the Tuareg from Timia Are Instrumentalizing Tourists to Support Their 'Exotic' Village," *In Tourism Development: Growth, Myths and Inequalities*, 39-51 (2008).

19. S. Khaydarova, and S. Khujamova, "The Vital Role of Libraries in Enriching Tourism Experiences," *Indian Journal of Information Sources and Services*, **14**(2), 11–16 (2024). https://doi.org/10.51983/ijiss-2024.14.2.02
20. O. Ulturgasheva, and M. Stelmaszyk, "Embracing Uncertainty: Porous and Actionable Responses to Climate Change at the Borders of Indigenous and Scientific Expertise(s) in Siberia," *Journal of the Royal Anthropological Institute* (2024).