

P4 - Cybersecurity in the tourism and hospitality industry. Critical issues and possible scenarios

2. DIGITAL TRANSFORMATION of ORGANIZATIONS and INDUSTRIES

Angelo Presenza¹ (presenza@unimol.it)

Myung Ja Kim² (silver@khu.ac.kr), Sergio Gil Moreno³ (sergio.moreno@ulpgc.es), Lorn Sheehan⁴ (Lorn@dal.ca)

¹ Department of Economic, University of Molise, Campobasso, Italy

² College of Hotel & Tourism Management, Kyung Hee University, Seoul, Republic of Korea

³ Facultad de Economía, Empresa y Turismo, Universidad de Las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Spain

⁴ Rowe School of Business, School for Resource and Environmental Studies, Dalhousie University, Halifax, Canada

Track summary: The spread of digital innovations such as cloud integration, customer analytics, connected devices, online transactions, and digital payment technology reveals that, by growing their digital footprint, hospitality and tourism (H&T) organizations are increasingly exposed to cyber threats commensurate with cyber-security as a critical contemporary issue. Problems range from data breach incidents that can potentially harm the companies' reputation and raise questions about consumers' privacy rights with the organizations to severe Information Technology infrastructure breakdowns.

For a clearer understanding of the extent of the phenomenon, consider that the average total cost of a data breach in the hospitality industry from 2021 to 2022 was \$2.94 million (Ponemon and IBM Security's 2022 global case study report).

Cybersecurity is not just about technology: it involves people and information, systems and processes, culture, and physical surroundings. The implication is that H&T organizations need to create a secure cyberspace for their employees, partners, suppliers, and customers and develop policies and practices that adequately manage threats or vulnerabilities.

Despite the significant concern about cyber-attacks in the H&T industry and the number of cybersecurity issues arising in both public and private organizations, there are surprisingly few studies addressing information security in the H&T management literature.

The scope of the Track is to advance the research of cybersecurity in the H&T industry creating a fertile arena for the theoretical advancement helpful to enhance academic understanding of this issue as well as for supporting stakeholders operating in this sector with new and helpful knowledge.