Cybersecurity and Data Protection

in the Hotel Industry

Student name: Fruzsina Valoczki

Student number: 2223630

Module name and code: Contemporary Themes in the Hotel and Hospitality Sector (BMIH6001)

Institution: University of Wales Trinity Saint David

Lecturer's name: Lola Villard-Coles

Date: 03/11/2025

I confirm that I have not used any AI tools in the research and creation of this assignment.

I confirm that I have not presented any AI generated materials as my own work.

I confirm I have copies of my drafts, notes, and other resources I used, which I may be asked to provide in evidence.

Research focus

Key causes of cybersecurity failures in hotels

Digitalisation

Improves efficiency but increases cyber risks

74% of hotels faced breaches, 45% had financial losses

Business impact

Cybersecurity is a strategic issue, not only IT

Protects guest data and maintains business trust

Case study focus

Based on global hotel chains

Highlights operational weaknesses and leadership response

(Anwar et al., 2024; Cahyandari et al., 2024)

Cyber Risk Factors in Hotel Operations

Key insights

01. Ransomware attacks can paralyse booking and payment systems

02. POS malware steals guests' payment information during transactions

03. Weak Wi-Fi security allows intruders to access hotel networks

04. Third-party suppliers increase exposure through connected systems

05. People remain the main source of breaches

06. Outdated IT slows threat detection and weakens security

07. Employees with limited awareness are more susceptible to manipulation

(Marino, 2025; Sharma, 2024)

Legal Framework

01.
- Guest data protection
- 72-hour breach report

02.
- Card payment security
- Encryption & access control

03.
- Up to €20M or 4% revenue

04.
- Audits, firewalls, encryption

05.
- Staff accountability & policy

06.
- Australia & U.S. state laws

07.
- Small hotels lack resources

(Hollander, 2020; Wolford, 2025; Pipyros & Liasidou, 2025; Hughes, 2025; Kirvan, 2024)

Reputation and Loyalty

Data breaches significantly reduce guest trust and brand reputation

Customer return rates may decline by up to 70%

Over 80% of travellers rely on online reviews

Transparent communication supports faster trust recovery

Ethical data governance promotes long-term customer loyalty

(Sutherland, 2025; Fan et al., 2021; Moon et al., 2022; Chotia et al., 2025)

Current Trends in Hotel Cybersecurity

Cybersecurity standards vary widely across hotels

Global chains invest millions in training, software & monitoring

Study of 100 small hotels: 27% train once a year, 28% offer none

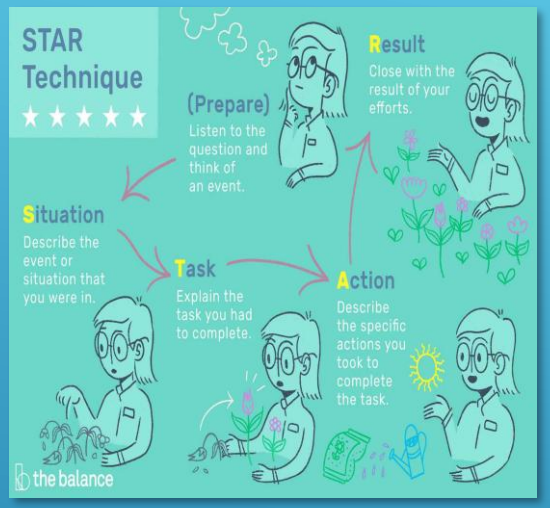
Reliance on third-party providers weakens defence

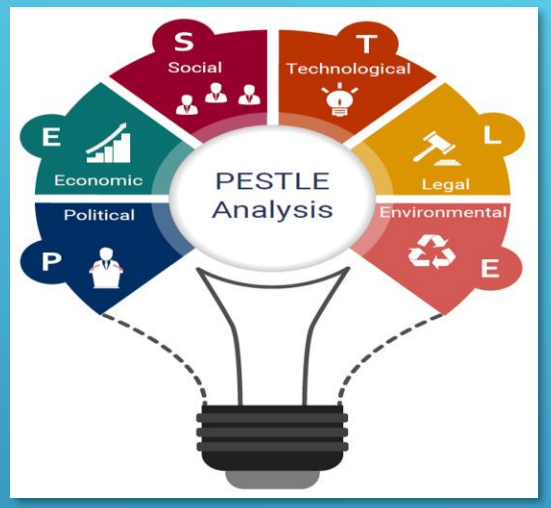
Security awareness lags digital transformation

The industry becomes stronger through cooperation and learning

(Source: Sharma, 2024)

Methodology and Analytical Framework





Qualitative research based on secondary data (2020–2025)

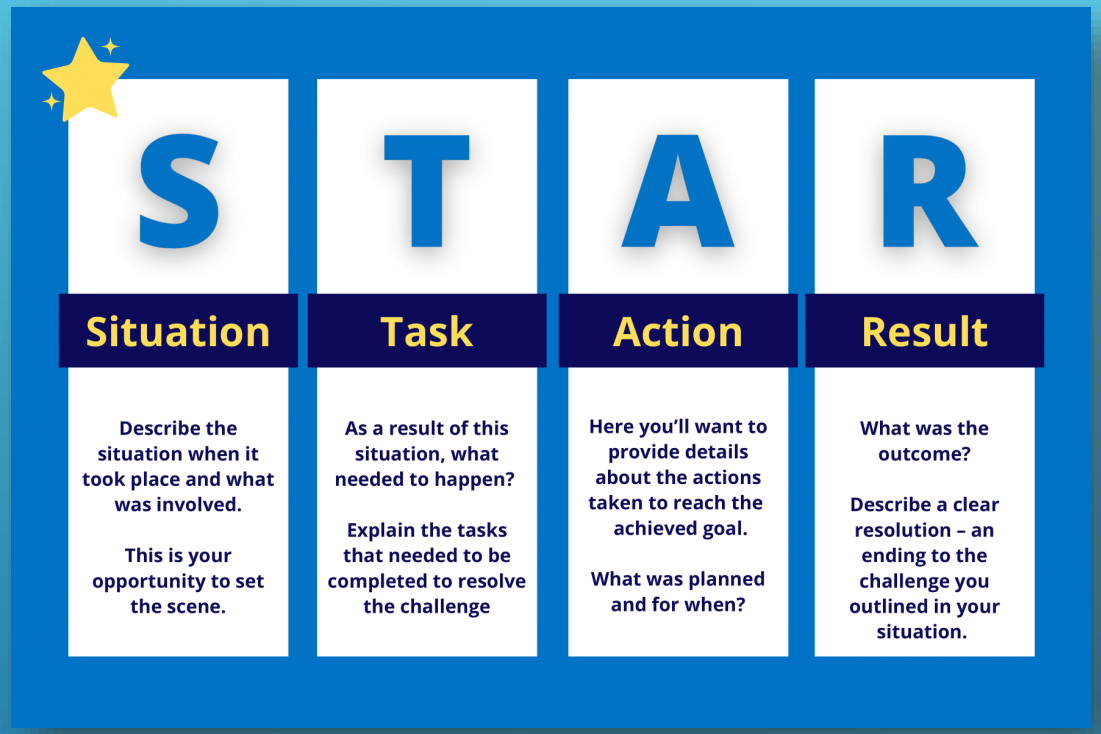
STAR framework used to analyse hotel cybersecurity incidents

Main PESTEL focus areas: technology, legal, and social aspects

Case studies: Marriott, MGM, Caesars, and Nordic Choice

Focus on organisational response, leadership, and resilience

Theme Impact Analysis



4 real-world cyber incidents analyse

Examined organisational response, leadership, and resilience

Focused on operational disruption, recovery, and long-term stability

Situation

Major Cyber Incidents in Global Hotel Chains

Operates over 225 hotels

In 2021, a ransomware attack shut down hotel operations

Operates nearly 9,400 properties

In 2018, a massive data leak revealed details of 500 million guests

In 2020, another breach revealed employee login information

Operates over 9,400 properties

In 2023, a phishing scam on LinkedIn targeted an MGM Resorts staff member

Operates 28 hotels

In 2023, a phishing call exposed loyalty members' data

Affecting around 10 million members

(Baker, 2022; Cole, 2023; Hammoudah & Ensign, 2025)

Task

Leadership and Organisational Challenges

Quick recovery and financial impact review after system failure

Managed legal duties, global notification laws, and reputation repair

Evaluated staff training, culture, and internal security awareness

(Bischoff, Garlington & Erdem, 2025; Bizga, 2021; Anishchuk, 2025; Hammoudah & Ensign, 2025)

Action

Organisational Responses to Cyber Incidents

Activated manual operations at 200 hotels

IT teams restored affected networks

Introduced multi-factor authentication

Customer support

Data deletion protocol

Offered complimentary credit monitoring

Refused ransom

Prioritised ethical recovery

Invested $30M in new security

Involved law enforcement

Offered credit monitoring

Verified that stolen data was erased

(Nair, 2025; Young, 2021; Okolie, 2025; Sayre, 2023; Brewer, 2023; Velotta, 2023)

Result

Impact by Hotel

Operations resumed

Limited long-term security improvement

Fined £18.4M (UK) & $52M (US)

Loss of customer trust and 5.6% share decline

$100M loss

Cancellations, guest frustration, reputation damage

2.7% share decline

Ongoing data protection weaknesses

(Collier, 2023; Page, 2020; Schwartz, 2023; Okolie, 2025; Hammoudah & Ensign, 2025; Brewer, 2023; Kilgore, 2018; Murphy, 2023; Kong, Kwan & Tong, 2022)

Conclusion

Building Long-Term Cyber Resilience

- Hotels must move beyond basic security compliance
- Strong protection = trained staff + responsible management + modern IT
- Continuous behavioural & organisational development needed
- Data protection = foundation of guest trust and brand reliability
- Strong leadership drives awareness and accountability
- Long-term resilience depends on collaboration between business, technology, and human factors

Building a Proactive Cybersecurity Culture

- Persistent human error and manipulation highlight the need for ongoing employee education
- Hotels must create a culture that consistently prioritises data protection
- Hilton’s annual programme shows strong results in preventing phishing incidents
- One yearly training cycle is not sufficient for high staff turnover environments
- Quarterly, role-specific sessions and simulated attacks improve awareness
- Regular training for all staff and business partners strengthens preparedness

(Hilton, 2024)

Upgrading Security Systems

- Cybersecurity modernisation requires replacing legacy and fragmented IT systems
- InterContinental Hotels Group adopted Fortinet SD-WAN for visibility and control
- Cloud security frameworks enable faster threat response and stronger defences
- Integrating advanced firewalls, detection, and event management systems improves scalability
- Partnering with security providers offers expert support

(Fortinet, 2023)

Access Control and Authentication

- Access control must include identity verification and privilege management
- Hyatt introduced biometric and password-free logins to reduce insider risks
- Multi-factor authentication (MFA) should be mandatory for all staff and partners
- Regular audits help detect outdated credentials and excessive access rights
- Restricting admin rights limits the damage of phishing attacks

(Hyatt, 2024)

Any Questions

THANKS
FOR YOUR
ATTENTION

References

1. Anishchuk, I. (2025) *An Analysis of Major Cybersecurity Failures: Case Studies of Target, Equifax, Yahoo, Marriott, and Capital One.* [online] Available at: https://doi.org/10.2139/ssrn.5427414 [Accessed: 26 October 2025].
2. Anwar, F.A., Deliana, D. and Suyamto, S. (2024) 'Digital Transformation in the Hospitality Industry: Improving Efficiency and Guest Experience', *International Journal of Management Science and Information Technology,* 4(2), pp. 428–437. Available at: https://doi.org/10.35870/ijmsit.v4i2.3201 [Accessed: 26 October 2025].
3. Baker, T. (2022) 'Here's How Nordic Choice Stopped a Ransomware Attack within Six Hours', *CoStar* [online]. Available at: https://www.costar.com/article/669022327/heres-how-nordic-choice-stopped-a-ransomware-attack-within-six-hours [Accessed: 17 October 2025].
4. Bischoff, J., Garlington, J. and Erdem, M. (2025) 'What Happens in Vegas No Longer Stays in Vegas—Cybersecurity Attacks on Las Vegas Integrated Resorts', *Journal of Hospitality & Tourism Cases* [online]. Available at: https://doi.org/10.1177/21649987251314898 [Accessed: 21 October 2025].
5. Bizga, A. (2021) 'Nordic Choice Hotels Confirm Ransomware Attack', *Bitdefender* [online]. Available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/nordic-choice-hotels-confirm-ransomware-attack [Accessed: 17 October 2025].

6. Brewer, R. (2023) 'Caesars: Driver's License, Social Security Data of Loyalty Members Stolen in Cyberattack', *Las Vegas Sun* [online]. Available at: https://lasvegassun.com/news/2023/sep/14/caesars-drivers-license-social-security-data-of-lo/ [Accessed: 25 October 2025].

7. Cahyandari, Y.P., Chusniyah, T. and Setiyowati, N. (2024) 'Cyber Resilience in Combating Ransomware Attacks: A Psychological Case Study Perspective on the Hospitality Industry', *INSPIRA: Indonesian Journal of Psychological Research,* 5(2), pp. 216–229. Available at: https://doi.org/10.32505/inspira.v5i2.9618 [Accessed: 29 September 2025].

8. Chotia, V., Khoualdi, K., Broccardo, L. and Yaqub, M.Z. (2025) 'The Role of Cyber Security and Digital Transformation in Gaining Competitive Advantage through Strategic Management Accounting', *Technology in Society,* 81, p. 102851. Available at: https://doi.org/10.1016/j.techsoc.2025.102851 [Accessed: 26 October 2025].

9. Cole, B. (2023) 'What MGM Resorts Attack Can Teach Small Businesses about Cybersecurity', *Forbes* [online]. Available at: https://www.forbes.com/sites/byroncole/2023/09/21/what-the-mgm-resorts-attack-can-teach-small-businesses-about-cybersecurity/ [Accessed: 13 October 2025].

10. Fan, W., Liu, Y., Li, H., Tuunainen, V.K. and Lin, Y. (2021) 'Quantifying the Effects of Online Review Content Structures on Hotel Review Helpfulness', *Internet Research*, 32(7). Available at: https://doi.org/10.1108/intr-11-2019-0452 [Accessed: 29 September 2025].

11. Fortinet (2023) *IHG Hotels & Resorts Boosts IT Efficiency Close to 60% with Fortinet Secure SD-WAN.* [online] Available at: https://www.fortinet.com/content/dam/fortinet/assets/case-studies/cs-ihg.pdf [Accessed: 1 October 2025].

12. Hammoudah, M. and Ensign, P.C. (2025) 'Vegas Cyber Attacks – A Natural Experiment in the Ransom Decision', *Journal of Teaching in Travel & Tourism,* pp. 1–11. Available at: https://doi.org/10.1080/15313220.2025.2544668 [Accessed: 25 October 2025].

13. Hilton (2024) *2024 Proxy Statement for Annual Meeting of Stockholders.* [online] Available at: https://stories-editor.hilton.com/wp-content/uploads/2024/04/2024-Proxy-Statement.pdf [Accessed: 22 October 2025].

14. Hollander, J. (2020) 'GDPR for Hotels: Here's What You Should Know (2022)', *Hotel Tech Report* [online]. Available at: https://hoteltechreport.com/news/data-protection-act [Accessed: 29 September 2025].

15. Hospitality Technology (2024) *Case Study: Yubico, Microsoft Deliver Strong Identity, Endpoint and Access Controls to Hyatt's Global Operations.* [online] Available at: https://hospitalitytech.com/case-study-yubico-microsoft-deliver-strong-identity-endpoint-and-access-controls-hyatts-global [Accessed: 27 October 2025].

16. Hughes, G. (2025) *Australia - Data Protection Law Guide - Law over Borders. Global Legal Post* [online]. Available at: https://www.globallegalpost.com/lawoverborders/data-protection-law-guide-1072382791/australia-1625858895 [Accessed: 6 October 2025].

17. Kilgore, T. (2018) 'Marriott's Stock Sinks After Disclosing Data Breach Affecting up to 500 Million Guests', *MarketWatch* [online]. Available at: https://www.marketwatch.com/story/marriotts-stock-sinks-after-disclosing-data-breach-affecting-up-to-500-million-guests-2018-11-30 [Accessed: 21 October 2025].

18. Kirvan, P. (2024) 'State of Data Privacy Laws in 2023', *TechTarget Security* [online]. Available at: https://www.techtarget.com/searchsecurity/tip/State-of-data-privacy-laws [Accessed: 3 October 2025].

19. Kong, A., Kwan, M. and Tong, L. (2022) *How to Design and Strengthen Cyber Security to Cope with Data Breach in the Hotel Industry? ResearchGate* [online]. Available at: https://www.researchgate.net/publication/360950915 [Accessed: 6 October 2025].

20. Marino, M. (2025) 'Cybersecurity Threats and Its Impact on the Hospitality Industry', *IJGHT* [online]. Available at: https://ijght.org/index.php/light/article/view/115/76 [Accessed: 8 October 2025].

21. Moon, H., Yu, J., Chua, B.-L. and Han, H. (2022) 'Hotel Privacy Management and Guest Trust Building: A Relational Signaling Perspective', *International Journal of Hospitality Management,* 102, p. 103171. Available at: https://doi.org/10.1016/j.ijhm.2022.103171 [Accessed: 20 October 2025].

22. Murphy, A. (2023) 'Caesars Entertainment Reportedly Paid Ransomware Demand', *Fox Business* [online]. Available at: https://www.foxbusiness.com/markets/caesars-entertainment-reportedly-paid-ransomware-demand [Accessed: 14 October 2025].

23. Nair, P. (2025) 'Nordic Choice Hotels, SPAR Stores Are Latest Attack Victims', *Data Breach Today* [online]. Available at: https://www.databreachtoday.com/nordic-choice-hotels-spar-stores-are-latest-attack-victims-a-18082 [Accessed: 13 October 2025].

24. Okolie, J. (2025) *A Cybersecurity Analysis of the Marriott International Data Breach of March 2020. ResearchGate* [online]. Available at: https://www.researchgate.net/publication/393716720 [Accessed: 13 October 2025].

25. Page, C. (2020) 'Marriott Hit with £18.4 Million GDPR Fine over Massive 2018 Data Breach', *Forbes* [online]. Available at: https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/ [Accessed: 13 October 2025].

26. Pipyros, K. and Liasidou, S. (2025) 'A New Cybersecurity Risk Assessment Framework for the Hospitality Industry: Techniques and Methods for Enhanced Data Protection and Threat Mitigation', *Worldwide Hospitality and Tourism Themes,* 17(1). Available at: https://doi.org/10.1108/whatt-12-2024-0296 [Accessed: 15 October 2025].

27. Sayre, K. (2023) 'MGM Resorts Refused to Pay Ransom in Cyberattack on Casinos', *The Wall Street Journal (WSJ)* [online]. Available at: https://www.wsj.com/tech/cybersecurity/mgm-resorts-refused-to-pay-ransom-in-cyberattack-on-casinos-3a53fa6d [Accessed: 19 October 2025].

28. Schwartz, C. (2023) 'How to Combat Hotel Data Breachers: A Guide for Independent Hoteliers', *Ehotelier* [online]. Available at: https://insights.ehotelier.com/insights/2023/01/31/how-to-combat-hotel-data-breachers-a-guide-for-independent-hoteliers/ [Accessed: 28 September 2025].

29. Sharma, D.S. (2024) Examination of Cybersecurity Practices in Small Hotels: A Comprehensive Study of Awareness, Challenges and Solutions. *University of Fairfax* [online]. Available at: https://www.academia.edu/126098448/Examination_of_Cybersecurity_Practices_in_Small_Hotels_A_Comprehensive_Study_of_Awareness_Challenges_and_Solutions [Accessed: 17 October 2025].

30. Sutherland, T. (2025) 'Data Breaches Affect Consumer Trust', *Security Magazine* [online]. Available at: https://www.securitymagazine.com/articles/101357-data-breaches-affect-consumer-trust [Accessed: 1 October 2025].

31. Velotta, R.N. (2023) 'Caesars Releases New Details on Cyberattack', *Las Vegas Review-Journal* [online]. Available at: https://www.reviewjournal.com/business/casinos-gaming/caesars-releases-new-details-on-cyberattack-2918145/ [Accessed: 7 October 2025].

32. Wolford, B. (2025) 'What Is GDPR, the EU's New Data Protection Law?', *GDPR.EU* [online]. Available at: https://gdpr.eu/what-is-gdpr/ [Accessed: 30 September 2025].

33. Young, K. (2021) *Cyber Case Study: Marriott Data Breach. CoverLink Insurance* [online]. Available at: https://coverlink.com/case-study/marriott-data-breach/ [Accessed: 4 October 2025].