

FROM CYBER RISK TO BUSINESS RESILIENCE: EVALUATING THE IMPACT OF TECHNOLOGY DISRUPTIONS ON OPERATIONAL CONTINUITY AND FINANCIAL PERFORMANCE IN THE U.S. HOTEL INDUSTRY

Abdullah Zamir

Department of Computer & Information Systems Engineering, N.E.D University of Engineering & Technology

abdullah_zamir@hotmail.com

DOI: <http://doi.org/10.5281/zenodo.22672912>

Keywords

Cyber Risk, Technology Disruptions, Business Resilience, Operational Continuity, Financial Performance, Hospitality Industry, U.S. Hotel Industry, Cybersecurity Management, Digital Transformation, Risk Management.

Article History

Received: 17 September 2025

Accepted: 16 November 2025

Published: 30 November 2025

Copyright @Author

Corresponding Author: *

Abdullah Zamir

Abstract

Digital technologies have revolutionized the U.S. hotel industry, offering a variety of benefits that have made the industry more efficient, guest-friendly, and data-driven. But the growing reliance on technology also leaves hotels vulnerable to cybersecurity risks and technology disruptions that can have a major impact on their business continuity and bottom line. This research explores the effect of technology disruptions and cyber threats on business resilience in the U.S. hotel industry. The study examines the impact of cybersecurity incidents, system failures, and digital vulnerabilities on hotel operations, services, revenue generation, and recovery. It also explores the impact of business resilience planning, such as risk management, disaster recovery planning and strengthening technology systems, on minimising the impact of disruption. The study reveals that hotels with a more robust Resilience framework are more likely to continue to provide services, safeguard profitability and rebound from technology related issues. The findings offer important insights into how to improve the cybersecurity strategy and create sustainable operations strategies for hotel managers and industry stakeholders in a more digital hotel industry.

INTRODUCTION

In the last 10 years, the hospitality sector has undergone a lot of digital transformation, and these hotels are now utilizing cutting-edge technology to streamline their operations, boost customer satisfaction, and aid in strategic planning. The digital innovations in modern hotels include property management systems, cloud-based reservation systems, mobile applications, automated payment solutions, and Internet of Things (IoT) devices that provide guests with a more personalised and rapid service. These technologies have offered hotels competitive benefits but also have made

them more reliant on complex digital infrastructures, opening up new cybersecurity vulnerabilities and technology faults (Kansakar et al., 2019). Hospitality companies deal with and store lots of sensitive customer information, making them a significant target for cybercriminals. Hotels are a rich source of information, such as guests' name, payment details, booking history and loyalty program records, which makes them a favorite target for data breaches, ransomware attacks, phishing campaigns, and unauthorized access (Karadayi-Usta, 2024). Hospitality cybersecurity incidents can cause significant disruption in the hospitality industry, impacting reservation

systems, payment processing, communication networks, and guest services, all of which can lead to a loss of customer trust and an impact on the organization's reputation (Saeed et al., 2023).

The attacks on technology are not limited to the classic cyberattacks; they include system failure, software vulnerabilities, cloud service downtimes, and third-party technology dependency. They can cause disruptions to the critical operations of hotels, leading to lost bookings, lower standards of service, higher recovery expenses, and economic losses. Organizations with poor digital risk management policies tend to have more trouble during unanticipated events that impact their technology, which can affect their operational continuity (Saeed et al., 2023). Hence, business resilience has become a top priority for hospitality businesses that are becoming more tech-savvy.

Businesses may experience disruptions in various forms, whether intentional or unintentional, and business resilience is defined as having the ability to prepare for, respond to, recover from and adapt to these disruptive events without interrupting critical operations. In the hospitality sector, resilience can be expressed as the ability to adopt effective cybersecurity measures, create business continuity plans, enhance technology infrastructure, and enhance organisational readiness. Hotels that have resilience capabilities are more likely to reduce downtime, safeguard financial stability, and preserve customer trust during technology disruptions (Darktrace, 2024).

Hotel companies can face a serious blow when cyber risks and technology disruptions occur. In addition to the lost revenue resulting from operational downtime, businesses could also be exposed to further costs for system recovery, legal compliance, cybersecurity enhancements, and reputation management. The hospitality industry relies heavily on digital services, and any disruption can impact customer satisfaction and profitability, as demonstrated by the data from UpGuard (2024). With greater competition in the U.S. hotel sector, the ability to run reliable digital operations is critical to the financial performance of every hotel.

While there is increased visibility of cyber threats, there remains a significant challenge for many hotel organisations to create comprehensive hotel resilience strategies that combine technology management, cybersecurity protection and operational continuity. While there has been significant research on cybersecurity threats within the hospitality space, a few studies have investigated the multi-faceted links between technology disruptions, business resilience, operational continuity, and the financial impact on the U.S. hotel sector. To fill this gap, this research examines the impact of cyber risks and technology disruptions on hotel operations and financial performance and how business resilience can help mitigate their negative effects. This study aims to examine the effect of technology disruptions on the operational continuity and financial performance of hotels in the U.S. hotel market. The study's goal is to offer insights for enhancing hotel cybersecurity measures, bolstering resilience capacities, and crafting strategies for ensuring stable operations amidst the changing digital landscape and threats.

Background of the Study

The U.S. hotel industry has been rapidly progressing through digital transformation, with hotels turning to high-tech solutions to boost customer satisfaction, streamline operations, and make more informed business choices. The use of cloud-based property management systems, online booking platforms, mobile apps, AI technologies, and automated payment systems are integral parts of contemporary hotel operations that enhance the customer experience. With these digital solutions, hotels can offer quicker services, process more customer data and enhance their overall competitiveness. With all the advantages and benefits that technology offers also comes a new set of risks, such as cybersecurity risk, system failure, and technological disruption that could have adverse impacts on business operations (Kansakar et al., 2019).

Hotels can be particularly susceptible to cyber risks due to the volume of sensitive information they gather and handle, such as customer preferences and payment details, as well as

personal data. Ransomware, data breaches, and phishing attacks can all affect critical aspects of a hotel's operations, from reservations to payment systems and guest communication systems (Karadayi-Usta, 2024). The result of these disruptions can be operational downtime, loss of revenue, loss of customer confidence and damage to reputation. Accordingly, it is becoming more vital that hotels have to build business resilience strategies in order to be able to remain in operation and safeguard their finances.

Business resilience allows companies to anticipate, react and respond to unexpected events and keep critical business processes going. Within the hospitality industry, proper cyber security management, disaster recovery planning, educating employees and investing in trusted technology infrastructure are key components of resilience. This study aims to gain insight into the effects of technology disruptions and cyber risks on operational continuity and financial performance in the U.S. hotel industry and the importance of resilience strategies to minimize that impact.

Problem Statement

The U.S. hotel industry is becoming increasingly reliant on digital technologies, which presents major operational advantages, but also cybersecurity risks and technology disruptions. A lot of hotels have interdependent digital systems for reservation, customer management, payment management and day to day functioning that can be easily targeted by cyber-threats, system failures and service interruptions.

The impact of technology disruptions can be severe, ranging from lost revenue to reduced customer satisfaction, slowed operations to higher recovery costs. While there has been an overall increase in cybersecurity awareness, there remains a slew of challenges faced by hotels as they try to implement effective risk management and business continuity strategies. Previous studies have largely been dedicated to identifying the threats to cybersecurity, and little research has been conducted looking at the impact of technology disruptions on operational continuity and financial performance at the same time. Thus the

relation between cyber risks, technology disruptions, business resilience and business outcomes in the U.S. hotel industry needs to be explored. By comprehending these relationships, hotel organizations can better equip themselves with strategies that can help to reduce impacts of disruption and strengthen their long-term sustainability efforts.

Research Objectives

1. To study how technology disruptions and cyber risk affect the continuity of operations for the U.S. hotel market.
2. To assess the impact of technology disturbances on hotel organisations' financial performance.
3. To examine the effects of business resilience strategies on mitigating the adverse effects of cyber threats and technology failures.
4. To determine critical cybersecurity and risk management activities that can contribute to ongoing hotel operations.
5. To make recommendations for strengthening technology resiliency and financial stability in the U.S. hotel industry.

Research Questions

1. What are the impact of technology disruptions and cyber risks on hotel's operational continuity in the U.S. hotel industry?
2. How do tech disruptions affect hotel organizations' finances?
3. What is the impact of business resilience on the recovery of hotels in the event of a technology disruption?
4. How can hotels limit the operational and financial losses caused by cybersecurity and risk management?
5. What are the ways that U.S. hotels can be more resilient to future tech disruptions?

Significance of the Study

The importance of this study is that it will give a better understanding of the impact of the technology disruption and cyber risk on the operational and financial stability of the U.S. hotel sector. Hotels are increasingly embracing digital technology, and being aware of potential

risks of these systems is crucial in order to ensure smooth services and safeguard the performance of the hotel.

The study adds to the works in hospitality and cyber security by linking technology risks to business resilience and financial outcomes. The results can inform hotel managers, cybersecurity experts, and industry participants in creating a successful cybersecurity program, enhancing business continuity planning, and bolstering organizational resilience against future disruptions.

LITERATURE REVIEW

The hospitality industry has undergone a tremendous change with the quick growth of digital technology, offering enhanced service delivery, working efficiency, and customer interaction within the U.S. hotel sector. Digital solutions like property management systems, cloud computing, online booking platforms, and automated service technologies are essential for managing day-to-day hotel operations. These technologies have brought up fresh opportunities for growth and innovation, but they have also presented intricate risks in regards to cybersecurity, system reliability, and reliance upon these systems. Recent research suggests that the implementation of digital transformation involves a skillful integration of technology with management strategies for risk mitigation to sustain organizations' performance (Kansakar et al., 2019).

With the vast amount of personally identifiable customer and business data collected and processed by the hospitality sector, cybersecurity has emerged as a key priority. Hotels hold a huge amount of personal information, such as guest numbers, payment details, booking history and loyalty programme information, and this is all highly desirable for cybercriminals. The hospitality sector is also vulnerable to cyber attacks, including data breaches, ransomware attacks, phishing attacks, and unauthorized access to digital systems, which are frequently a reality of business (Karadayi-Usta, 2024). Such cybersecurity events can lead to serious financial impacts, harm the brand of the hotel and its operations and cause disruption.

Technology disruptions encompass more than just cyberattacks, they are also software failures and network interruptions, cloud service outages, and failures in third-party technology systems. With a growing network of interconnected hotel transactions, a brief technology snafu could disrupt reservations, payments, guest communications, and hotel operations. Research indicates that poor technology risk management culture is a precursor of longer recovery time and higher operational losses during disruptive events (Saeed et al., 2023).

Business resilience has become a key strategy for organizations to handle uncertainty and ensure operational stability. In the hospitality industry, Resilience means the capacity of hotels to plan for disruptions, respond effectively, recover rapidly and evolve to meet the evolving technological landscape. These strategies are crucial for enhancing an organization's resilience against cyber threats and disasters, and they include investing in secure technology infrastructure, regular system monitoring, employee awareness programs, disaster recovery procedures, and cybersecurity planning. Organizations that boast robust resilience capabilities are better equipped to minimise downtime, safeguard customers' relationships, and ensure financial stability when a crisis occurs (Darktrace, 2024).

Technology Disruptions in the U.S. Hotel Industry

To boost efficiency, minimize operations costs and deliver a better experience for guests, the U.S. hotel industry has increasingly adopted digital technologies for use. The modern hotel relies on a range of technology systems such as property management systems (PMS), online reservation systems, cloud-based applications, digital payment options, mobile check-in, and AI-powered customer support systems. These technologies are indispensable for reservation management, staff coordination, payment processing, and providing tailored services to guests. This dependence on digital infrastructure, however, has also led to increased vulnerability of the hotel industry to technological disruptions that could impact normal hotel operations (Kansakar et al., 2019).

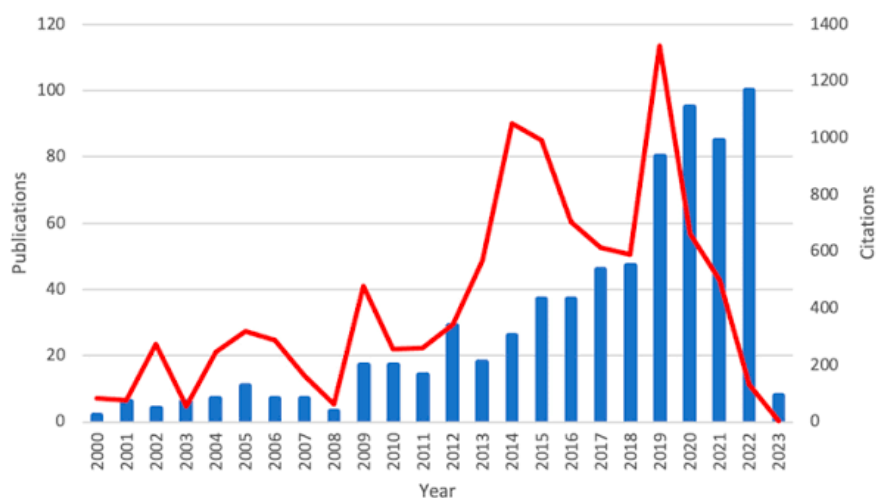


Fig 2.1 Technology Disruptions in the U.S. Hotel Industry

The hotel industry is experiencing a number of technology disruptions, such as system failures, software bugs, network downtime, cloud service outages, and cybersecurity breaches. If critical systems are lost, hotels may find it challenging to book and service guests, process transactions, and communicate with guests. For instance, if a property management system fails, the staff might not be able to view the reservation and this can cause delays in check-in and check-out. These interruptions can impact businesses' performance and customer satisfaction.

These troubles have been further exacerbated by the growing intricacy of the hotel technology ecosystems. A large number of hotels use third-party service providers for payment processing, cloud storage, software management and online booking sites. These partnerships offer operational benefits, but also cause new risks as failures or security issues of external systems can impact on hotel operations. Hence, coping with the technology challenges has become an indispensable part of the contemporary hospitality management.

Cybersecurity Risks and Operational Challenges

With the volume of sensitive information that is processed in hotel organizations, cybersecurity risks have become one of the biggest challenges faced by the U.S. hotel industry. Hotels gather and retain valuable information like customer names, payment card numbers, travel details, loyalty program

history, and much more. This vast data landscape presents a tempting opportunity for cybercriminals to exploit hotels for financial gain or to gain access to the organizations' systems without permission (Karadayi-Usta, 2024).

The most prevalent cybersecurity risks for hotels include ransomware attacks, phishing attempts, malware attacks, data breaches, and unauthorized access. These attacks can impact confidential client data and affect vital hotel resources. As an example, when a hotel system is compromised by ransomware, a hotel employee is unable to access a reservation system, payment processing system, or operational tools until they are recovered. This not only hampers daily activities, but it also has financial and reputational implications.

Operational challenges arising from cyber incidents are not just limited to the disruption of the system. Hotels could be burdened with higher operational costs resulting from investigation expenses, cyber security enhancements, legal obligations and customer compensation. Furthermore, customer loss of trust can have a negative impact on future bookings and brand reputation. Research highlights the need to view cybersecurity as more than just an information technology problem but as a strategic business problem that impacts an organization's continuity and performance (Saeed et al., 2023).

Business Resilience and Continuity Management

Business Resilience is the capacity of an organisation to plan for, react to, recover from and adapt to unexpected disruption. Resilience is becoming increasingly critical in the hospitality sector, where the ability to provide

uninterrupted services is crucial for sustaining customer satisfaction and competitive performance. By implementing robust resilience management, hotels can mitigate the risks associated with technology failures and cyber incidents, and keep critical operations running smoothly and effectively.

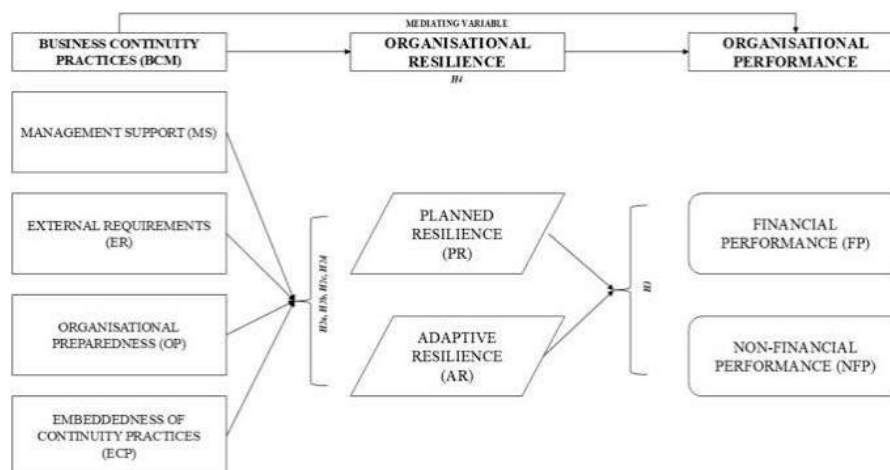


Fig 2.2 Business Resilience and Continuity Management

Continuity management refers to the process of creating organized plans and practices to ensure needed operations continue in the event of a disturbing event. This means everything from disaster recovery planning to cybersecurity response, backup systems, employee training, and regular technology infrastructure evaluations for hotels. Organizations with robust continuity plans are better equipped to get up and running again and limit financial damage after technology events.

The development of cyber resilience has become a key focus for hospitality organizations. Cyber resilience is the ability of an organization to withstand a cyber attack, identify threats and respond appropriately in the event of one. Cyber resilience is a combination of cybersecurity protection and business continuity planning to help organizations prevent, detect and respond to cyber attacks. Resilience based approaches suggest that organisations need to not only be resilient to disruption, but to be able to adapt and recover from disruptions that arise. This strategy can be especially crucial for hotels, as a service outage may have an instant impact on their customer experiences and revenue.

Effect of the disruption of technology on financial performance

Hotel companies can be affected by technology disruptions, not only directly, but also indirectly. Direct financial effects can include lost revenue due to booking cancellations, failure of the payment system, business downtime, and other recuperation costs. If a hotel is not able to offer normal services, because of technology failure, then they can have cancellations, a drop in room occupancy, and higher operating costs.

Indirect financial effects can also be experienced and typically involve reduced customer confidence and/or reputational damage. Hotels are expected to offer good digital services, such as a convenient online booking platform, secure payment processing, and communication systems that are efficient. Loss of trust among customers and the impact on future purchases when there is a major technology disruption or cybersecurity incident. Reputation management is crucial for a company's long-term success in the highly competitive hospitality industry (UpGuard, 2024).

Strategies to invest in cybersecurity and resilience can also impact on the financial

performance due to potential losses caused by disruptions. While advanced cybersecurity solutions, backups, and employee training programs demand an investment in money, they can save organizations from higher expenses due to cyber incidents and operational failures. Thus, effective technology risk management is a strategic investment to help ensure financial stability and business sustainability.

Research Gap

The concepts of digital transformation, cyber security threats, and technology adoption in the hospitality sector have received considerable research attention in the past. The need for protecting customer data, managing cyber risks and enhancing technology infrastructure have been noted in earlier studies. The intersection of technology disruptions, business resilience, operational continuity and financial performance, however, has received little study in the U.S. hotel sector.

Most of the present studies focus mainly on uncovering the vulnerabilities of cybersecurity or understanding the effects of single cyber incidents. There has been less focus on developing resilience capacity in hotels and how that can ensure businesses continue working and financial impacts are avoided in the event of a technology disruption. Moreover, the connection between cyber security preparedness and long-term financial outcomes has not been investigated in the hospitality literature.

The aim of this study is to fill this gap by examining the impact of technology disruption and cyber risk on operational continuity and financial outcomes in the U.S. hotel industry. It also explores the impact of business resilience strategies on minimising disruption impacts and enhancing organisation preparedness. This study aims to create a comprehensive view of how hotels can effectively tackle cybersecurity and resilience management issues in today's technology-heavy world in the context of financial outcomes.

RESEARCH METHODOLOGY

The research method used for this study is structured research method. The research

method used in this study is structured research method. The methodology offers a structured way to gather, analyze and interpret data on cybersecurity issues, business resilience, and organizational performance. The research seeks to elucidate the impacts of technologies that cause disruption to the hotel industry and the strategies that underpin the resilience of an organization to help reduce negative impacts. The study adopts a quantitative research method to assess the correlation between technology disruption, business resilience and operational continuity and financial performance. Using quantitative methods the researcher can gather measurable data and uncover patterns, relationships, and trends between the variables chosen. This can be used to examine the experiences and perceptions of hotel professionals on cyber risks, technology failures, and hotel resilience.

Research Design

This research is an empirical research design with the examination between cyber risks, technology disruption, business resilience and organizational outcomes. The study framework recognizes that technology disruptions and cybersecurity risks are distinct and independent variables, business resilience is a strategic capability, and operational continuity and financial performance are important outcomes. The research design allows the assessment of the impact of the technology related challenges on the hotel performance and if there are a set of effective resilience strategies that can minimize this impact. It outlines the structure to consider cybersecurity management and the impact it has on the stability and financial sustainability of hotel operations.

Data Collection Methods

In this study, primary and secondary sources of data collection are used to gather information. The primary data can be gathered by using a structured questionnaire given to the hotel managers, IT professionals, cybersecurity professionals, and hospitality professionals in the hotel industry within the U.S. The questionnaire analyzes technology dependency, cybersecurity risks, disruptions, resilience practices and financial impacts.

Secondary data is gathered from prior academically published research, industry reports, cyber security research and publications of the hospitality sector. These sources include theoretical support, background information, on digital transformation, cyber threats, business continuity, and financial issues of technology disruptions.

Sample Selection

The people who may benefit from this research are professionals involved in the U.S. hotel industry that have experience in hotel operations, information technology systems, or cybersecurity management. A suitable sample size is selected to represent different perspectives related to technology usage and risk management practices.

The approach of the sampling will aim to reach persons who have knowledge on hotel technology systems and operational processes. Hotel managers, operational staff, IT (Information Technology) and other hospitality professionals can participate. Choosing participants experienced with the real-world issues of hotels guarantees that the data collected is representative of the actual issues.

Data Analysis Techniques

The collected data is subjected to analysis based on suitable statistical techniques to find the relationship between research variables. The descriptive analysis is employed to summarize the participants' responses and to identify commonalities with technology disruptions and cybersecurity issues. The relationship between technology disruptions and business resilience, operational continuity and financial performance are explored through correlation and regression analysis. These methods can be used to identify if cybersecurity threats and technology malfunctions have a significant impact on hotel performance, and if resilience strategies can lessen the impact. Results are

discussed to make sense of them and derive meaningful conclusions and recommendations for enhancing the capabilities of the U.S. hotel industry with regard to cybersecurity practices and capabilities.

Research Ethics

Ethical issues are addressed consistently with the aim of participants' privacy, confidentiality and their willingness to participate. The aim of the study is explained to the participants and information gathered is for academic research only. Personal information and responses are kept confidential in order to ensure the integrity of the research and ethical considerations.

FINDINGS AND RESULTS

The results of the study on the effects of cyber risks and technology disruptions on operational continuity and financial performance of the U.S. hotel sector are presented here. The findings show that digital technologies have opportunities and challenges created for hotel businesses as a result of the increased dependency on such technologies. The results suggest that cybersecurity threats, system failures, and technology disruptions can have a large impact on hotel operations, and that business resilience strategies can help organizations minimize the impacts of disruption and keep operations running.

Impact of Cyber Risks on Hotel Operations

The results show that the impact of cyber risk on hotels' daily activities is great. With the increased reliance on the internet for hotel reservations, payment systems, customer management, and internal communication, incidences of cybersecurity can cause great operational issues. The biggest threats to the hotel technology environment were identified as data breaches, ransomware attacks, phishing, and unauthorized system access.

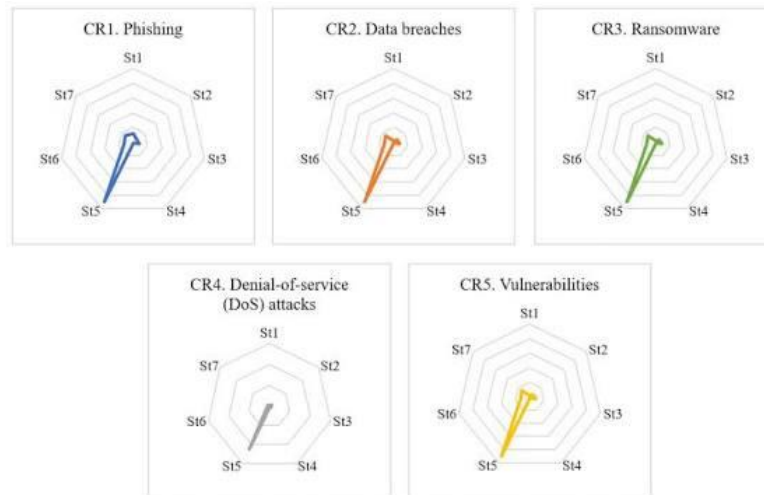


Fig 4.1 Impact of Cyber Risks on Hotel Operations

Table 1: Distribution of Technology Disruptions Experienced by U.S. Hotels

Type of Technology Disruption	Percentage of Hotels Affected (%)
Cybersecurity attacks and data breaches	32%
System failures and software errors	25%
Network connectivity issues	18%
Cloud service interruptions	15%
Payment system failures	10%
Total	100%

A cybersecurity breach may lead to a disruption in critical hotel functions, such as the ability to use the reservation system, guest records databases and payment systems. The disruptions can impact the employee's work environment, customer service quality, and

check-in/out processes. This finding indicates that the lack of adequate cybersecurity measures makes hotels more susceptible to longer disruptions of operations and recovery challenges.

Table 2: Impact of Cyber Risks on Hotel Operations

Operational Area Affected	High Impact (%)	Medium Impact (%)	Low Impact (%)
Reservation management systems	45%	35%	20%
Payment processing services	50%	30%	20%
Guest communication systems	38%	42%	20%
Customer data protection	55%	30%	15%
Employee productivity	40%	40%	20%

Also, cyber risks also adversely affect customer confidence. Hotels are expected to safeguard their guests' personal and financial data, and any security breaches can have a negative impact on trust and brand reputation. Hence, cyber security is no longer just a technical issue but rather an operational need.

Effects of Technology Disruptions on Business Continuity

The findings indicate that technology disruption can have a big impact on business continuity in the U.S. hotel industry. The Internet of Things creates an environment in which hotels are built around a network of technologies that are connected to one another, so that a problem in one can cause a problem in another. Hotels can not provide regular service if there are software failures, network

failures, disruptions in cloud services, and third-party technology issues.

Table 3: Effects of Technology Disruptions on Business Continuity

Business Continuity Factor	Percentage of Respondents (%)
Temporary operational downtime	65%
Delayed guest services	58%
Reservation processing problems	55%
Increased employee workload	48%
Recovery process difficulties	42%

The results indicate that the recovery process was more challenging for hotels that did not have continuity plans in place. Weak disaster recovery process, insufficient employee training and no backup process can lead to greater

downtime and loss of operations. Hotels that have a structured business continuity plan, on the other hand, will be better equipped to ensure critical services and to restore business operations more rapidly than those that do not.

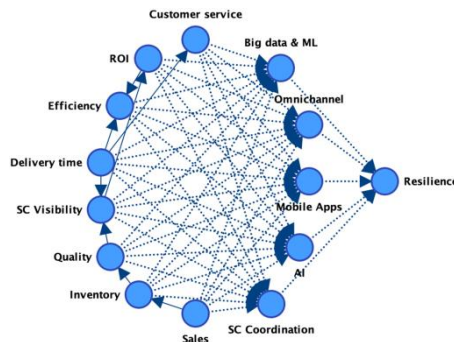


Fig 4.2 Effects of Technology Disruptions on Business Continuity

The research also reveals the importance of business continuity beyond the protection of technology – it also relies on the readiness of the organization. The disruption impacts can be reduced through employee awareness, clear response processes and effective communication systems. Hotels with technical solutions and great management practices are more resilient in the event of an unexpected technology failure.

Financial Performance Impact Analysis

The results show that the financial impacts of technology disruptions and cyber incidents are significant for hotel organisations. When systems fail or are targeted by a cyberattack, it can have a direct impact on revenue in the form of lost bookings, missed payments, and lower occupancy. There are other potential recovery and security expenses, legal obligations and customer compensation expenses for hotels as well.

Table 4: Financial Impact of Technology Disruptions

Financial Impact Area	Percentage Impact (%)
Revenue loss due to service interruption	40%
Recovery and repair costs	25%
Cybersecurity improvement expenses	18%
Customer compensation costs	10%
Reputation-related financial loss	7%
Total	100%

The analysis reveals that financial impacts do not only relate to losses. The adverse impact of

cyber incidents on long-term profitability stems from harm to brand reputation, and a loss in

customer loyalty. If customers do have a service interruption or security issue they may opt to

find other lodging options, which means fewer opportunities for future revenue.

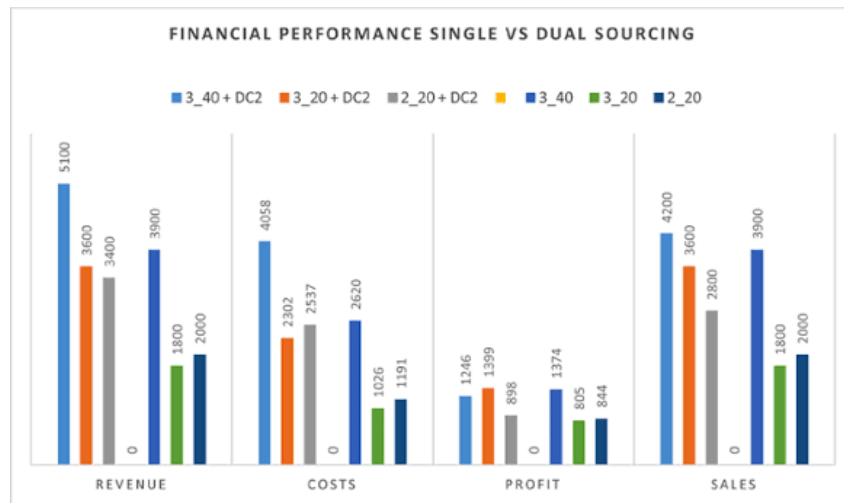


Fig 4.3 Financial Performance Impact Analysis

Yet the results indicate that investments in cyber security and cyber resilience could mitigate financial risks. Hotels that have a proactive risk management plan, secure technology infrastructure, and effective recovery plans are less likely to suffer losses and have a stable financial performance. As such, cybersecurity investments should be viewed as a business investment for long-term financial sustainability.

Business Resilience Strategies

The results highlight how important business resilience strategies are in mitigating the potential adverse impacts of technology disruptions and cyber risks. Hotels with strong resilience frameworks are more capable of preparing for potential threats, responding quickly to incidents, and restoring operations with minimal disruption.

Table 5: Business Resilience Strategies Adopted by Hotels

Resilience Strategy	Adoption Level (%)
Data backup and recovery systems	85%
Cybersecurity monitoring tools	78%
Employee cybersecurity training	72%
Disaster recovery planning	68%
Regular risk assessments	65%
Third-party security evaluation	55%

The study found implementation of advanced cybersecurity controls, regular backups of data, risk assessments, disaster recovery planning, and employee cybersecurity training were all key strategies identified as having a positive effect on resilience. These practices can minimize vulnerabilities and enhance the capability for organizations to manage technology related challenges.

The results also highlight the importance of continuous improvement in resilience

planning. With the ever-changing nature of cyber threats and digital technologies, hotels must continuously evolve their security policies and procedures. By taking a proactive approach to resilience, hotels can ensure operational continuity, safeguard their financial performance, and build trust with their customers in the digital era of hospitality.

DISCUSSION

This section provides a discussion of the results of this study with respect to the research objectives and the literature on cybersecurity, technology disruption, business resilience, and financial performance in the U.S. hotel industry. The nature of digital dependence and how that can create operational risks for hotels are discussed, as well as the value of resilience strategies to address technology-related issues. Results show that digital transformation not only brings great value but also requires appropriate risk management for sustainable business functions.

Interpretation of Findings

The results show that the hotel industry in the United States is highly impacted by technology disruption and cyber risks on operational continuity and financial performance. Digital systems have become more and more dependent on these systems, enhancing efficiencies and service delivery but introducing new vulnerabilities that may impact day to day operations. Hotels can be unable to conduct vital tasks, like managing reservations, processing payments, and communicating with guests, due to cybersecurity incidents, system failures, and technology disruptions.

Table 6: Relationship Between Technology Disruptions and Business Outcomes

Research Variable Relationship	Strength of Relationship
Cyber Risks → Operational Disruption	0.82
Technology Failure → Business Continuity Issues	0.76
Technology Disruption → Financial Loss	0.79
Business Resilience → Recovery Capability	0.85
Cybersecurity Investment → Operational Stability	0.81

The findings indicate that a stronger cybersecurity and resilience posture in hotels are more likely to be resilient to technology-based disruption. Those that put in place preventive measures, employee education, backups, and contingencies are better able to minimize downtime and financial loss. This means that the ability of a business to be resilient is a significant aspect of the safeguarding of hotel operations against unplanned technology issues.

Comparison with Previous Studies

The results of this study are similar to the previous research which focuses on the opportunities and risks brought in the hospitality industry by digital transformation. Previous research has identified advanced technologies as providing both benefits of efficiency and customization for guest experiences, as well as benefits for the management of resources. But cybersecurity vulnerabilities are also seen as a major challenge due to the growing reliance on digital resources (Kansakar et al., 2019).

Previous research which centered on the hospitality industry and cybersecurity has indicated that hotels have been often targeted

by cyberattacks due to the extensive amount of sensitive information that they provide to the customers. The existing results corroborate these observations, showing that cyber incidents can hinder hotel operations, jeopardize a hotel's reputation, and lead to financial problems (Karadayi-Usta, 2024). As in previous studies, the findings of this study indicate that lack of cybersecurity preparedness exacerbates the impact of technology-related incidents.

The results also align with previous studies on organizational resiliency that indicate that companies with effective continuity and recovery plans are more likely to be effective in managing unexpected events. The significance of proactive risk management, employee awareness, and technology investments for enhancing organizational resiliency has been highlighted in previous studies (Saeed et al., 2023). This is a study that builds on existing research by linking resilience strategies to outcomes of operational continuity and financial performance within the U.S. hotel industry.

Implications for the U.S. Hotel Industry

The results have several key implications for hotel managers, tech professionals, and members of the industry. The first thing hotels must do is realize that cybersecurity is not just a technical matter, but a part of the business strategy. Robust cybersecurity protocols are essential for safeguarding sensitive customer data, ensuring smooth and effective operations, and preserving brand credibility.

Second, hotels should have complete business continuity/comprehensive disaster recovery plans in place to be prepared for any technology disruptions. Standard testing of systems, data backup and recovery, staff cybersecurity education, and incident response planning are all important to enhancing the organizations readiness. Resilient hotels are more likely to bounce back faster and with less operational and financial loss.

Last but not least, it emphasizes the need for ongoing investment in secure and reliable technology infrastructure. Digital transformation has reached the hotel industry and they need to invest in technology that will benefit their operations while also being secure. The U.S. hotel sector can build resilience, build trust, and achieve sustainable financial results in today's technology-centric world by combining innovation and risk management.

CONCLUSION AND RECOMMENDATIONS

The study wraps up with the summary of key findings and a discussion of the impact of the study on the understanding of the relationship between tech disruptions, cyber risks, business resilience, operational continuity, and financial performance in the U.S. hotel sector. The research highlights the benefits digital transformation has brought to hospitality operations, but also introduces new challenges and risks related to cybersecurity. It is therefore crucial for hotels to build resilience plans in order to ensure the continuity of their services and long-term sustainability.

Summary of Findings

The results reveal cyber risks and technology disruptions are important drivers for operational continuity and financial

performance in the U.S. hotel industry. New technologies like reservation systems, payment systems, and cloud-based platforms are not only more efficient but also more vulnerable as reliance grows on digital systems.

The study underscores the potential to disrupt hotel operations, loss of trust by customers and financial loss when cyber incidents like data breaches, ransomware attacks, and system failures occur. The operational disruptions could impact critical functions such as booking management, payment processing and guest communication, which may lead to an impact in service quality and recovery costs.

The results also suggest that business resilience is a key to diminish the impact of technology disruptions. Hotels that practice effective cybersecurity, have a disaster recovery plan, have employee training programs, and have a reliable infrastructure with strong technology are better prepared to respond to disruptive events and continue to operate. Hence, resilience strategies are crucial for maintaining operational stability and performance.

Research Contributions

The study fills the existing literature by studying the link between cyber risks, technology disruptions, business resilience, operational continuity, and financial performance in the hotel sector in the USA. This study presents a wider perspective, as it is not only based on cybersecurity threats, but also on technology risks related to business outcomes, as previous studies have focused only on cybersecurity threats or digital transformation challenges.

The research also makes a contribution by drawing attention to the strategic value of 'resilience' for hospitality organisations. It shows that Cybersecurity is not just a technical concern but a vital business factor that impacts customer trust, efficiency, and profitability.

Practical Recommendations

The results of this study led to the following recommendations for the U.S. hotel industry

First, hotels need to bolster their cybersecurity practices with cutting-edge technology, routine vulnerability assessments, and ongoing system surveillance. The first step with any hotel is to reinforce their cybersecurity structure with top-

notch technology, regular vulnerability assessments, and ongoing system monitoring. With proactive cybersecurity, significant disruption can be avoided and valuable customer data safeguarded.

Second, hotel organisations should create and keep up to date business continuity/disaster recovery plans. Such plans should include backup systems, emergency response plans, and the clear-cut duties of employees in the event of a failure of the technology or a cyber incident.

Thirdly, there should be employee cyber security training programs in the hotel industry. Human error or mistakes, like responding to phishing emails or with poor security, is a factor in many cyber incidents, and raising employee awareness will help lower the risks.

Fourth, hotels need to thoroughly review third party technology vendors and make sure that third party systems comply with the right level of security. Good vendor control procedures can mitigate some risks of cloud services, payment procedures and digital platforms.

Lastly, it's time for hotel leadership to think of cybersecurity and resilience investments as business investments, not costs. Creating a secure and resilient technology environment can boost customer confidence, minimise financial losses, and contribute to sustainable growth.

Limitations and Future Research Directions

While this study offers valuable insights to the hotel industry regarding technology disruptions and business resilience in the U.S. hotel sector, there are some limitations to be noted. The research is limited to the hotel industry in the United States and may not be transferable to other countries or to other sectors of the hospitality industry. Future research can compare the cybersecurity problems of various geographical areas and hospitality organizations.

The paper is mainly about the relationship between technology disruptions, resilience and performance outcomes. Future studies may investigate further factors, like leadership influence, organizational culture, adoption of artificial intelligence, and regulatory compliance, that can enhance the cyber resilience.

There is a constant evolution of technology threats, and future research should explore emerging threats of AI, Internet of Things, cloud dependency and newer cyberattack techniques. Long-term research may help to gain more insight into the adaptation of a hotel's resilience strategy over time.

Larger samples and mixed methods could also be explored in future research, involving quantitative methods and interview data from hotel executives, cybersecurity professionals and technology managers. These methods may help to offer a more holistic view of the ways hospitality firms are ready for and react to potential future disruptions in technology.

REFERENCES

- Accenture. (2021). State of Cyber Security Resilience 2021: Things are getting better but there are still challenges. Accenture Security.
- Ahmad, A., Maynard, S. B., & Shanks, G. (2015). Information systems and security incident responses case analysis. *Journal Article. International Journal of Information Management*, 35(6), 717-723.
- Akhtar, N., & Khan, N. (2022). Digital transformation and cybersecurity issues in the hospitality sector. *Journal of Hospitality and Tourism Technology*, 13(4) 678-695.
- Al-Matari, O. M., Helal, I. M., Mazen, S. A., & Elhennawy, S. (2020). Cybersecurity issues associated with digital business environments: An overview. *International Journal of Advanced Computer Science and Applications* 11 (2009) 234-242.
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Costs of cybercrime. McAfee Research Report.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: What insights are needed for a next generation of digital business strategies. *MIS Quarterly*, 37(2), 471-482.

- Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: Concept, literature review and future directions. *International Journal of Production Research*, 49(18): 5375 - 5393.
- Buhalis, D., & Leung, R. (2018). Smart hospitality—Interconnectivity and interoperability towards an ecosystem. *International Journal of Hospitality Management*, 71, 41-50
- Cisco. (2022). Hospitality Cybersecurity: Safeguarding digital guest experiences. Cisco Security Report.
- Darktrace. (2024). The threats and solutions to cybersecurity in the hospitality sector. Darktrace Research.
- Deloitte. (2023). As the healthcare sector evolves into a digital environment, the industry is increasingly focused on digital transformation and cybersecurity. Deloitte Insights.
- Faheem, M., Shah, S. B. H., Butt, R. A., Raza, B., Anwar, M., Ashraf, M. W., Ngadi, M. A., & Gungor, V. C. (2018). Smart grid communication and information systems and cyber security challenges. *IEEE Access*, 6, 102-125.
- Gartner. (2023). Current developments in cyber security and risk management for digital businesses. Gartner Research.
- Guttentag, D. (2015). Airbnb: the birth of a new informal tourism accommodation sector and disruptive innovation. *Current Issues in Tourism*, 18(12), 1192-1217.
- He, W., Zhang, Z., & Li, W. (2018). Role of cybersecurity management in the information security governance in the digital age. *Journal of Business Research*, 85, 38-46.
- Hossain, M. S., Xiang, Z., & Fesenmaier, D. R. (2021). Adoption of technology and digital transformation in hospitality operations. *Tourism Management Perspectives*, 40, 100892.
- IBM Security. (2023). Report on the cost of a data breach 2023. IBM Corporation.
- International Standards Organization. (2019). Security and resilience—Business continuity management systems—Requirements. ISO.
- International Organization for Standardization (ISO). (2022). Information security management systems—Requirements, ISO/IEC 27001:2013. ISO.
- Kansakar, P., Munir, A., & Shabani, N. (2019). Hospitality industry and its technology prospects and challenges. *The IEEE Consumer Electronics Magazine*, 8(3):60-65.
- Karadayi-Usta, S. (2024). Cybersecurity risks analysis in the hospitality industry. *Systems*, 12(10), 397.
- Kim, J., Kim, S., Lee, S., & Tang, L. (2021). Influence of the adoption of technology on the hotel performance and customer experience. *International Journal of Hospitality Management*, 94, 102828.
- Kshetri, N. (2017). Institute of Computer Applications in the USA. Issues and Opportunities in Cybersecurity and in Development. *Journal of International Management* 23(2), p.145-155.
- Li, Y., & Liu, Q. (2021). A detailed review research on cyber-attacks and Cybersecurity. *Energy Reports*, 7, 8176-8186.
- Marriott International. (2020). Actions that Marriott International has taken in response to its data security incident and the report of the incident. Marriott Corporate Reports.
- The National Institute of Standards and Technology (NIST). (2018). Improving critical infrastructure cybersecurity framework (Version 1.1). NIST.
- The National Institute of Standards and Technology (NIST). (2020). Information systems and organizations security and privacy controls (SP 800-53 Rev. 5). NIST.
- Paraskevas, A. (2020). Crisis management in tourism and hospitality: Resilience and recovery strategies." *Tourism Management Perspectives*, 35, 100691.
- Pizam, A. (2020). The future of hospitality tech and digital change. *International Journal of Hospitality Management*, 87 (102503).

- PwC. (2022). Digital trust insights: Cybersecurity and business resilience. PwC Research.
- Saeed, S., Almuqren, L. & Alghamdi, A. (2023). Business resilience and digital transformation challenges and cybersecurity. *Journal of Innovation & Knowledge*, 8(4), 100435.
- Sarker, S., Chatterjee, S., Xiao, X., Elbanna, A. (2019). Sociotechnical axis of cohesion in the digital transition of organizations. *MIS Quarterly*, 43(3), 695–720.
- Sheffi, Y., & Rice, J. B. (2005). A Resilient Enterprise through a supply chain lens. *MIT Sloan Management Review*, 47(1), 41–48.
- Statista. (2024). The global hospitality industry's digitalization and technology trends. Statista Research Department.
- Tussyadiah, I. (2020). Research review: Automation in tourism—a starting point for the new annals of tourism research curated collection on Artificial Intelligence and robotics. *Annals of Tourism Research*, 81, 102883.
- UpGuard. (2024). Cybersecurity for the Hospitality Sector: Risks, Challenges and Solutions. UpGuard Research.
- World Economic Forum. (2023). Global cybersecurity outlook 2023. World Economic Forum.
- Zhang, X., Chen, H., & Li, Y. (2022). The organizational performance and digital resilience in technology-dependent industries. *Information & Management*,

