ISSN: 2634-9221
European Journal of Applied Sciences; Vol. 14 No. 04 (2026) (375-384)
https://doi.org/10.14738/aivp.1404.12100

Small Hotels, Big Consequences: How Cyberattacks Undermine Economic and Defense Systems

Swati Sharma and Timothy Godlove

1. American National University, Virginia, USA

Abstract: Cyberattacks targeting small hotels have intensified in both scale and sophistication, exposing a critical but often overlooked vulnerability within the hospitality sector. Although these establishments operate with limited resources, they process large volumes of guest data, maintain internet-connected operational systems, and increasingly rely on automated property management platforms. This combination creates an attractive attack surface for cybercriminals and generates consequences that extend far beyond individual businesses. This article examines how cyberattacks against small hotels disrupt local economies, damage community trust, and weaken the resilience of interconnected commercial and governmental systems. Using analysis of recent hospitality incidents, industry reports, and cyber-physical system risks, particular attention is given to regional and national defense implications because hotels frequently support military personnel, defense contractors, and government travelers. The analysis highlights how vulnerabilities in small hospitality environments can cascade into broader security challenges. The study concludes with actionable recommendations for hotel operators, vendors, policymakers, and educators to strengthen cyber readiness, improve technology governance, and reduce systemic risk in this critical yet underserved segment of the hospitality industry.

Keywords: cybersecurity, hospitality, hotels, economic resilience, national defense, cyber-physical systems

INTRODUCTION

Cybersecurity risks now extend beyond the conventional high-value domains of banking, government, and telecommunications. Over the past decade, adversaries have deliberately widened their focus to encompass sectors that may appear less critical at first glance but are, in fact, deeply interwoven with economic resilience and national infrastructure. Among these, the hospitality industry—and particularly small to mid-sized hotels—has emerged as a vulnerable and increasingly exploited attack surface. At the level of individual properties, such hotels may seem too modest in scale to attract sophisticated cybercriminals or state-backed actors. However, when considered collectively, they form a vast, interconnected digital ecosystem that extends far beyond front-desk operations. Their reliance on reservation platforms, online payment gateways, guest Wi-Fi, and Internet of Things (IoT) infrastructure creates a web of digital dependencies that intersect with financial institutions, international travel networks, and even defense-related mobility. The routine presence of government officials, business executives, and contractors within these establishments amplifies the strategic value of hotels as both opportunistic targets for cybercrime and potential nodes for espionage. In this sense, small and mid-sized hotels occupy a paradoxical position: they are insignificant in isolation but collectively systemically significant. The underinvestment in cybersecurity across this sector, therefore, represents

not merely a business risk but a structural weakness with implications for both global economic stability and national security.

The stakes are high. According to recent reports, more than 30% of hotels globally experienced a data breach in the past year, with the majority of those properties suffering repeat incidents within months of the first attack [1]. These figures underscore that hotels are far from being incidental or low-value targets; instead, they represent recurring entry points within the broader landscape of cybercrime. The consequences of such vulnerabilities extend well beyond the immediate boundaries of the hospitality sector. A successful breach not only disrupts hotel operations but also triggers cascading effects across interconnected regional tourism economies, undermining business continuity for restaurants, transport providers, and local attractions that rely heavily on visitor inflows.

Equally concerning is the erosion of public trust in digital financial systems when payment platforms associated with hotels are compromised. Guests who experience fraud or data theft during their travels may become hesitant to engage in online transactions, thereby diminishing consumer confidence at a systemic level. Beyond economic repercussions, hotels also pose a national security risk, as they are frequented by diplomats, defense contractors, and corporate leaders, making them attractive targets for surveillance by adversaries. In these contexts, hotels can unintentionally serve as operational vectors for espionage campaigns, data exfiltration, or even infiltration into defense-related digital ecosystems [6]. This article examines why small hotels are appealing cyber targets, the economic consequences of attacks, the implications for national security and cyber-physical systems, and selected hospitality-sector incidents. It then presents practical mitigation and policy recommendations for hotel operators, vendors, industry associations, and policymakers.

RELATED WORK AND SECTOR CONTEXT

Recent scholarship and primary industry research identify hospitality organizations as attractive cyber targets because digital transformation has increased their dependence on interconnected reservation, payment, guest-network, cloud, and Internet of Things (IoT) systems. Karadayi-Usta's hospitality-sector risk analysis emphasizes the exposure created by digitization and the need to evaluate cybersecurity across multiple stakeholders [2]. Trustwave's 2025 hospitality-sector assessment similarly documents a large external attack surface, legacy services, exposed systems, and tens of thousands of identified vulnerabilities [3]. Hospitality-specific IoT research further shows that smart rooms, sensors, actuators, and other connected services introduce security, privacy, and ethical concerns because guests interact directly with these technologies and generate substantial amounts of data [4].

Operational research also demonstrates that cyber incidents can produce prolonged business disruption. VikingCloud's 2025 survey of North American hotel IT and security leaders found that 82% of surveyed hotels experienced a successful cyberattack during the 2024 summer season and that 44% experienced more than 12 hours of downtime [5]. At the strategic level, the DarkHotel campaign demonstrates that compromised hotel networks can be used to target selected travelers. At the same time, cyber-physical systems research explains how compromise of connected digital components can create consequences in physical environments [6], [7]. Together, these sources establish a stronger scholarly and

primary-source foundation for examining small hotels as economically important but comparatively under-resourced cybersecurity environments.

REVIEW METHOD

This article uses a focused narrative review and case-analysis approach based on recent incidents, industry reports, and cybersecurity sources cited in the manuscript. The analysis organizes the available evidence around four themes: attack surface and data value, economic consequences, national security and cyber-physical implications, and practical mitigation. Three hospitality incidents are used as illustrative cases to show how operational disruption and supplier risk can extend beyond a single property. This approach is intended to synthesize the cited evidence and derive practical recommendations; it is not presented as a systematic review or an experimental study.

FINDINGS

Why Small Hotels Are Appealing Targets

Small hotels are attractive targets for cybercriminals because they combine extensive digital connectivity, valuable guest information, and comparatively limited cybersecurity resources. Their dependence on reservation systems, payment platforms, wireless networks, and increasingly connected building technologies expands the potential attack surface.

At the same time, smaller properties often lack dedicated cybersecurity personnel, mature security programs, and strong vendor-management practices. The following sections examine three primary factors contributing to this vulnerability: accessibility and attack surface, the value of hotel data, and weaknesses in existing defenses.

Accessibility and Attack Surface

Small hotels rely heavily on digital systems to manage reservations, process payments, provide Wi-Fi access, and increasingly control physical infrastructure such as smart locks and HVAC systems. Each of these platforms creates a potential point of vulnerability. Unlike larger chains, smaller operators often lack in-house IT teams or comprehensive vendor oversight, leaving them disproportionately exposed. Guest-facing technologies remain prominent exposure points, including payment and point-of-sale systems, guest Wi-Fi, and front-desk systems [5].

Data Richness and Value

Hotels are custodians of dense personal datasets that may include government-issued identification, payment card information, loyalty account data, and detailed travel itineraries. The compromise of these records creates substantial privacy and fraud risks [3], [4].

Weak Defenses

Cost pressures often lead small hotels to operate on outdated or legacy systems that may not receive timely security updates. Trustwave's 2025 hospitality-sector analysis identified 95,040 vulnerabilities, including 14,318 classified as critical and 1,521 associated with the U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities catalog [3]. Training gaps compound the problem: front-desk staff, who interact daily with external queries, may also face phishing and social-engineering attempts.

Economic Consequences

Direct Costs of Breaches

The financial burden of cyber incidents is substantial. Hospitality-sector reporting places the average cost of a hospitality data breach at approximately USD 3.62 million in 2023 and USD 3.86 million in 2024 [3]. While such averages are influenced by organization size, losses of this magnitude illustrate why cyber incidents can be proportionally severe for smaller operators with narrower margins.

Operational Disruption

Operational impacts can be substantial. VikingCloud's 2025 hospitality research found that 82% of surveyed North American hotels experienced a successful cyberattack during the 2024 summer season. Among successfully breached hotels, 44% reported more than 12 hours of downtime [5].

Reputational Erosion and Spillover

Trust is central to hospitality. Cyber incidents can damage guest confidence, generate negative reviews, and reduce occupancy. In VikingCloud's hospitality survey, reputational damage from negative reviews was the most frequently cited potential business impact, while respondents also identified financial losses, lawsuits, and lower occupancy [5].

Insurance and Compliance Costs

Cyber incidents can also increase insurance, legal, compliance, and notification burdens. In VikingCloud's hospitality survey, 30% of respondents identified higher insurance premiums as a likely business impact of cyberattacks [5].

Table 1 summarizes selected, directly traceable quantitative findings from hospitality-sector and primary sources [3], [5], [8].

Table 1: Selected Verified Cybersecurity Impacts in the Hospitality Sector. Sources: [3], [5], [8].

Impact / Indicator	Verified Evidence	Source
Average hospitality data breach	$3.62M (2023); $3.86M (2024)	[3]
North American hotels reporting successful cyberattack, summer 2024	82%	[5]
Hotels reporting >12 hours downtime after attack	44%	[5]
MGM Resorts estimated September 2023 impact	Approx. $100M negative impact to Adjusted Property EBITDAR	[8]
MGM Resorts one-time incident expenses	Less than $10M	[8]
Critical vulnerabilities in Trustwave hospitality analysis	14,318 critical; 1,521 in CISA KEV	[3]

Defense and National Security Implications

Hotels as Espionage Vectors

Hotels are frequented by diplomats, defense contractors, and executives from industries with sensitive information. The DarkHotel campaign demonstrated how compromised hotel networks could be used to target selected travelers and deliver malicious software to high-value guests [6].

Cyber-Physical Threats

As hotels adopt Internet of Things (IoT) devices, intrusions increasingly blur the line between data theft and physical disruption. Smart rooms, connected sensors, access-control technologies, surveillance systems, and building-management devices expand the cyber-physical attack surface and create security and privacy concerns unique to hospitality environments [4], [7].

Weak Links in National Cyber Defense

Hotels can therefore represent a weak link that adversaries may exploit to target sensitive individuals or establish opportunities for further compromise, as demonstrated by campaigns such as DarkHotel [6].

CASE ANALYSIS

MGM Resorts Breach (2023)

The 2023 cyberattack on MGM Resorts, although involving a large operator, demonstrates the operational and financial consequences that can follow a major hospitality-sector compromise. MGM reported system shutdowns and disruptions at affected properties, exposure of certain customer personal information, an estimated USD 100 million negative impact to Adjusted Property EBITDAR, and less than USD 10 million in one-time incident expenses [8].

Otelier Supply-Chain Breach (2024)

Otelier, a hotel-management technology provider used across major hospitality brands, experienced unauthorized access beginning in July 2024. Reporting in January 2025 indicated that attackers accessed cloud storage containing hotel guest information and reservation data, illustrating how compromise of a shared technology provider can propagate risk across numerous properties and brands [9].

BWH Hotels Reservation Data Breach (2026)

In April 2026, BWH Hotels disclosed unauthorized access to a web application containing guest reservation data. The exposed information included names, contact information, reservation numbers, dates of stay, and special requests, while payment and banking information were reportedly not involved. The incident illustrates how internet-facing hospitality applications can expose travel-related information useful for follow-on phishing and social-engineering activity [10]. Table 2 summarizes the selected incidents used in the case analysis.

Table 2: Selected Cybersecurity Incidents in the Hospitality Sector.

Year	Incident	Description	Broader Impact
2023	MGM Resorts	Cyber incident disrupted systems and exposed certain customer personal information.	Approx. $100M estimated EBITDAR impact; regulatory and litigation consequences [8].
2024–2025	Otelier supply-chain breach	Cloud storage compromise exposed hotel guest and reservation information across major brands.	Demonstrated third-party and shared-platform risk [9].
2026	BWH Hotels reservation-data breach	Web-application compromise exposed contact and reservation information.	Demonstrated risk from internet-facing hospitality applications and follow-on phishing [10].

DISCUSSION

The evidence reviewed in this article indicates that the cybersecurity significance of small hotels is disproportionate to the size of any individual property. Their combination of sensitive guest information, payment systems, third-party platforms, guest networks, and increasingly connected physical systems creates multiple paths for compromise. The economic effects include direct recovery costs, downtime, reputational damage, and increased insurance and compliance burdens. At the same time, the presence of government personnel, defense contractors, diplomats, and business leaders creates an additional security dimension that extends beyond ordinary commercial risk.

The case examples also illustrate the importance of interconnectedness. The MGM Resorts incident demonstrates the operational and financial consequences that can follow a major compromise [8]. The Otelier case demonstrates how supplier and shared-platform vulnerabilities can propagate across multiple hospitality organizations [9]. The BWH Hotels incident illustrates the continuing exposure of internet-facing reservation applications and the sensitivity of travel-related data [10]. These patterns support treating hospitality

cybersecurity as a shared resilience issue involving operators, vendors, industry associations, insurers, policymakers, and educators.

This analysis has limitations. It relies on the published and publicly available sources cited in the manuscript and uses selected incidents as illustrative cases rather than a comprehensive dataset. Consequently, the conclusions should be interpreted as a synthesis of the cited evidence and a basis for practical risk-reduction recommendations rather than as estimates derived from a systematic review or controlled empirical study.

MITIGATION AND POLICY RECOMMENDATIONS

For Hotel Operators

Network Segmentation: Hotels should adopt network segmentation practices, separating guest Wi-Fi from internal operational systems such as reservation platforms, financial databases, and building management software. This reduces the likelihood that a compromise of one system will cascade across the entire network infrastructure. These measures align with the risk-management and protective-control practices emphasized in the NIST Cybersecurity Framework 2.0 [11].

Multi-Factor Authentication (MFA): Administrative accounts and privileged access points should be protected with multi-factor authentication. MFA significantly decreases the risk of unauthorized access by requiring attackers to compromise more than just a stolen or weak password. CISA likewise recommends MFA as a core cybersecurity practice for small and medium-sized organizations [12].

Routine Patching and Asset Management: Maintaining an up-to-date inventory of digital assets and promptly applying security patches are essential to minimizing exposure to known vulnerabilities. Cybercriminals often exploit legacy or unpatched systems as an easy entry point. Asset inventory and timely vulnerability remediation are consistent with NIST CSF 2.0 and CISA small-business guidance [11], [12].

Offline Backups and Incident Response Readiness: Regularly maintained offline backups ensure that critical operational data can be restored in the event of ransomware or data corruption. Equally important is testing incident response plans so that staff know exactly how to act during an active breach, minimizing downtime and financial loss. Tested recovery and incident-response capabilities are central resilience practices in NIST CSF 2.0 [11].

Comprehensive Staff Training: Since human error remains one of the most common causes of breaches, training employees to recognize phishing attempts, social engineering tactics, and suspicious online behavior is crucial. Well-trained employees serve as an important line of defense against malicious intrusions. CISA guidance for small and medium-sized businesses also emphasizes employee awareness and phishing resistance [12].

For Vendors and Industry Associations

Standardized Vendor Security Requirements

Hotels should establish and enforce uniform cybersecurity requirements for all third-party vendors, including providers of reservation platforms, payment systems, and property

management software. Standardization ensures that all suppliers adhere to baseline security practices, reducing the likelihood that a weak link in the supply chain becomes an entry point for cyberattacks.

Regular Supplier Audits

Conducting systematic, annual security audits of technology vendors and service providers helps verify compliance with security standards and uncovers vulnerabilities before they can be exploited. These audits create accountability across the supply chain and allow hotels to take corrective action when risks are identified.

Hospitality-Specific Information Sharing and Analysis Centers (ISACs)

The formation of ISACs tailored to the hospitality sector would allow hotels, suppliers, and industry associations to exchange real-time threat intelligence. By pooling insights and incident data, these centers strengthen collective awareness, accelerate responses to emerging threats, and provide small operators with access to resources that would otherwise be unavailable to them.

For Policymakers

Financial Incentives for Cybersecurity Investments

Governments can play a pivotal role in strengthening hotel cybersecurity by offering subsidies, grants, or tax incentives that offset the costs of upgrading digital infrastructure. Such measures are particularly critical for small and medium-sized hotels, which often operate on limited budgets and may otherwise postpone essential security improvements.

Tailored Compliance Frameworks for SMEs

Instead of applying one-size-fits-all regulations, policymakers should develop compliance frameworks specifically designed for small and medium-sized enterprises (SMEs) in the hospitality sector.

These frameworks should strike a balance between practicality and security, ensuring that requirements are achievable without imposing undue financial or administrative burdens.

Recognition of Hospitality as Part of Critical Infrastructure

Given the sector's intersection with finance, tourism, and national security, cybersecurity in hospitality should be integrated into broader critical infrastructure protection strategies.

By doing so, hotels—especially those located in politically or economically strategic regions—would gain access to national defense resources, intelligence sharing, and emergency response coordination in the event of cyberattacks.

CONCLUSION

At first glance, small hotels may appear peripheral to national or corporate cybersecurity strategies, yet their vulnerabilities can have ripple effects far greater than their size might suggest. These establishments are custodians of sensitive customer data, including payment credentials, personal identification, and travel itineraries. They also function as interconnected nodes within global mobility and tourism networks, where a single breach can disrupt supply chains and erode consumer trust. Beyond the economic dimension, hotels—frequented by business leaders, diplomats, and defense contractors—can serve as inadvertent staging grounds for espionage and intelligence gathering, amplifying their significance as potential targets. The evidence reviewed in this article suggests that overlooking the cybersecurity posture of small and mid-sized hotels can undermine the resilience of regional economies while creating broader risks for national security. Addressing this challenge demands a comprehensive, multi-stakeholder approach. Hotel operators must strengthen operational defenses, vendors must enforce rigorous security standards across the supply chain, insurers should incentivize the adoption of best practices, and policymakers should integrate hospitality into critical infrastructure protection frameworks. Only through such a holistic strategy can the sector's systemic vulnerabilities be effectively mitigated, closing a gap that adversaries have increasingly learned to exploit.

REFERENCES

[1] OysterLink, "Hospitality cybersecurity: 2026 threats and trends," updated Oct. 29, 2025. [Online]. Available: https://oysterlink.com/spotlight/cybersecurity-hospitality-industry/

[2] S. Karadayi-Usta, "Cybersecurity risks analysis in the hospitality industry: A stakeholder perspective on sustainable service systems," Systems, vol. 12, no. 10, p. 397, 2024, doi: 10.3390/systems12100397.

[3] Trustwave, "2025 Trustwave Risk Radar Report: Hospitality Sector," 2025. [Online]. Available: https://www.trustwave.com/hubfs/Web/Library/Documents_pdf/2025_Trustwave_Hospitality_Risk_Radar.pdf

[4] S. Mercan, K. Akkaya, L. Cain, and J. Thomas, "Security, privacy and ethical concerns of IoT implementations in hospitality domain," in Proc. IEEE 13th Int. Conf. Internet of Things (iThings), 2020, pp. 198–203, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00048.

[5] VikingCloud, "Peak season, peak risk: The 2025 state of hospitality cyber report," July 9, 2025. [Online]. Available: https://www.vikingcloud.com/resources/peak-season-peak-risk-the-2025-state-of-hospitality-cyber-report

[6] Kaspersky Lab, "The Darkhotel APT: A story of unusual hospitality," Global Research & Analysis Team, 2014.

[7] Y. Z. Lun, A. D'Innocenzo, I. Malavolta, and M. D. Di Benedetto, "Cyber-physical systems security: A systematic mapping study," arXiv:1605.09641, 2016, doi: 10.48550/arXiv.1605.09641.

[8] MGM Resorts International, "Current Report on Form 8-K," U.S. Securities and Exchange Commission, Oct. 5, 2023. [Online]. Available: https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm

[9] L. Abrams, “Otelier data breach exposes info, hotel reservations of millions,” BleepingComputer, Jan. 17, 2025. [Online]. Available: https://www.bleepingcomputer.com/news/security/otelier-data-breach-exposes-info-hotel-reservations-of-millions

[10] E. Kovacs, “BWH Hotels says hackers had access to reservation data for 6 months,” SecurityWeek, May 12, 2026. [Online]. Available: https://www.securityweek.com/bwh-hotels-says-hackers-had-access-to-reservation-data-for-6-months/

[11] National Institute of Standards and Technology, “The NIST Cybersecurity Framework (CSF) 2.0,” NIST CSWP 29, Feb. 2024, doi: 10.6028/NIST.CSWP.29.

[12] Cybersecurity and Infrastructure Security Agency, “Cyber guidance for small and medium businesses,” U.S. Department of Homeland Security. [Online]. Available: https://www.cisa.gov/audiences/small-and-medium-businesses