Flight delays and cancellations due to airport technology network disruptions worldwide

Sirikorn Loedlukthanathan[1], Thongchai Jeeradist[2]*

Chandrakasem Rajabhat University[1] , Aviation Personnel Development Institute, Kasem Bundit University[2]

Received: 20 July 2024

Revised: 26 August 2024

Accepted: 30 August 2024

Abstract

This paper discusses the growing issue of flight delays and cancellations resulting from airport technology network disruptions on a global scale. As airports become increasingly reliant on complex technological systems to manage operations, the risks associated with network failures, cyberattacks, and other disruptions have escalated. These disruptions can incapacitate critical infrastructure such as communication systems, baggage handling, passenger processing, and air traffic control. The consequences are multifaceted, including operational inefficiencies, significant financial losses, compromised security, and a negative impact on passenger experience. This review identifies and categorizes the primary causes of airport technology network disruptions, including cybersecurity threats, technical failures, natural disasters, and human errors. Notably, the increased sophistication of cyber threats, as highlighted by reports from cybersecurity firms like CrowdStrike, poses a severe risk to airport operations. The findings emphasize the importance of implementing robust cybersecurity measures, enhancing network redundancy, conducting regular security audits, and developing comprehensive incident response plans.

Keywords: Flight delays and cancellations, Airport technology, Network disruptions

*Corresponding Author: Email: thongchai.jee@kbu.ac.th

Introduction

Disruptions in airport technology networks can lead to significant delays and cancellations of flights, impacting both airlines and passengers. This review article focuses on the causes, effects, and possible solutions for mitigating these disruptions. Flight delays or cancellation in airline operations caused by technology network, which includes scheduling flights, assigning gates, and managing crews, will cause disruptions as well as passenger information systems will struggle to provide updates about flight statuses, delays, and gate changes.

Information Technology (IT) network failure is potentially devastating in technology-driven businesses such as, technical failures in hardware malfunctions, software outdated, malicious software or “Malware” of Spyware, Trojan, Backdoor, Virus or Worm (Electronic Transactions Development Agency, 2021) can lead to failures in the airport's information technology infrastructure. It’s cause travelers might not get up-to-date or correct information about their flights. Airports are increasingly becoming targets for cyber-attacks or Cybersecurity Breaches, which can disrupt communication systems, flight information displays, and operational software. Together with hardware malfunctions, technical failures or outdated systems can lead to failures in the airport's information technology infrastructure. Human error or mistakes by information technology personnel of improper maintenance, or configuration errors can also result in network disruptions. Furthermore, natural disaster such as typhoon, hurricanes, earthquakes, power outages, or construction work can disrupt airport networks as external factors. The congestion or overload can affect network performance. Airlines and Airport operators must implement measures that will enable them to remain their flight operations during such events and must implement security measures such as firewalls, regular virus scans, and authentication processes to protect their networks. Software errors in configured systems, including hardware compatibility issues and configuration conflicts, can impede network functions. While regular updates of software and hardware support minimize this risk. Additionally, rigorous testing of system functionality should be conducted to identify and resolve any potential issues. By focusing on these areas, the aviation industry can enhance its ability to manage and mitigate the impact of network disruptions, ensuring smoother and more reliable airport operations.

By leveraging insights and solutions from companies like CrowdStrike, airports can strengthen their defenses against cyber threats, ensuring safer and more reliable flight operations.

Objective

To study the impact of airport technology network disruptions on flight delays and cancellations worldwide, utilizing insights and data from CrowdStrike to understand the role of cybersecurity threats in these disruptions.

Introduction to Airport Technology Networks and Their Importance

Airport technology infrastructure in airport operations, the critical role of technology networks including communication systems, flight information displays, baggage handling systems, and security systems. These networks must be ensured the smooth coordination of flights, passenger processing, and security.

The airport information technology system become highly reliant on IT systems and digital technologies for operational efficiency, safety, and customer service. This dependency increases the risk and impact of network disruptions.

Airport technology network disruptions refer to incidents where the digital infrastructure that supports airport operations is compromised, leading to operational issues. These disruptions can result from technical failures, cyberattacks, or human error, affecting communication systems, flight information displays, baggage handling, security systems, and more.

CrowdStrike, a leading cybersecurity company, frequently publishes insights on cyber threats, including those affecting the aviation industry. They often analyze the impacts of cyberattacks on airport technology networks, which can lead to flight delays and cancellations.

Key points relevant to airport technology network disruptions and how CrowdStrike's insights and expertise may apply.

Impact of Network Disruptions

1) Flight Delays and Cancellations: Disrupted communication systems can prevent proper coordination between airlines, air traffic control, and ground services, leading to delays and cancellations.

2) Passenger Experience: Passengers face inconveniences such as missed connections, long wait times, and lack of information about their flights

3) Operational Efficiency: Airlines and airports may incur additional costs for rescheduling flights, accommodating stranded passengers, and handling customer complaints.

4) Security Risks: Disruptions can compromise security systems, making it challenging to monitor and manage access control, baggage handling, and other critical operations.

Types of Cyber Threats to Airport Technology Networks

1) Ransomware Attacks: Cybercriminals may deploy ransomware to lock critical systems, demanding payment to restore access. These attacks can disable key airport systems, leading to operational shutdowns.

2) Distributed Denial of Service (DDoS) Attacks: By overwhelming airport IT infrastructure with excessive traffic, DDoS attacks can cripple systems that handle flight scheduling, baggage handling, and security checks.

3) Phishing and Social Engineering: These attacks can target airport staff, tricking them into providing access credentials, leading to breaches in secure systems.

Impact of Cyberattacks on Flight Operations

1) Disrupted Communications: Cyberattacks can take down communication systems between airlines, air traffic control, and ground services, making it difficult to coordinate flights.

2) Compromised Flight Information Systems: Systems displaying flight statuses might show inaccurate information, leading to confusion and mismanagement of flight operations.

3) Grounding Flights: Severe attacks may force airlines to ground flights to prevent potential safety issues caused by compromised systems.

Impact on Service Quality and Passenger Experience

1) Passenger dissatisfaction by network disruptions that lead to long wait times, flight delays, or canceled flights can cause significant frustration among passengers. The inconvenience can result in negative reviews, complaints, and a reluctance to use the affected airport in the future.

2) Loss of Confidence in Airport Systems by repeated disruptions can erode passenger confidence in the reliability and safety of airport systems. This can lead to anxiety about travel and reluctance to fly, particularly among business travelers who value reliability.

Enhancing Airport Cybersecurity and Resilience

Adopt Advanced Cybersecurity Solutions by encourage airports to implement advanced cybersecurity tools like CrowdStrike's Falcon platform, which offers comprehensive endpoint protection, threat intelligence, and automated response capabilities. Integrate with A-CDM Systems: Suggest the integration of cybersecurity measures with Airport Collaborative Decision Making (A-CDM) systems to improve coordination and response during cyber incidents. This can help ensure real-time sharing of threat information and better manage disruptions (Jeeradist, 2023). Airports should have well-defined incident response plans to quickly address network disruptions. Regular drills and simulations should be conducted to ensure preparedness. Regularly audit and assess airport information technology systems to identify vulnerabilities and ensure compliance with cybersecurity standards. This includes penetration testing and vulnerability scanning. Train airport staff on cybersecurity best practices, phishing detection, and how to respond to suspicious activities. A well-informed workforce is a critical defense against social engineering attacks. Establish partnerships with cybersecurity firms to leverage their expertise in threat intelligence, incident response, and cybersecurity strategy development.

CrowdStrike’s Insights on Aviation Cybersecurity

Reports and Publications: Review CrowdStrike’s annual Global Threat Reports and other publications focusing on cyber threats in aviation. These reports provide data on the frequency and type of attacks, as well as specific insights into the tactics used against airport networks.

Case Studies and Success Stories: Explore case studies where CrowdStrike’s solutions have helped airports and airlines protect against cyber threats, respond to incidents, and recover from disruptions. These examples can provide practical insights into the effectiveness of advanced cybersecurity measures.

APT Groups Targeting Aviation: CrowdStrike tracks Advanced Persistent Threat (APT) groups, including those targeting the aviation sector. Understanding the methods and motivations of these groups can help airports strengthen their defenses.

CrowdStrike's 2024 Global Threat Report highlights several critical cybersecurity trends impacting the aviation sector and beyond. The report identifies a significant increase in sophisticated cyber threats, including a 75% rise in cloud intrusions and a marked shift towards malware-free attacks. Attackers increasingly rely on valid credentials and legitimate tools to avoid detection, making it challenging for defenders to distinguish between normal user behavior and malicious activity. These techniques allow adversaries to gain quick and often unnoticed access to sensitive systems

The report also notes a concerning rise in identity-based attacks, often facilitated by generative AI technologies. Adversaries are leveraging social engineering, SIM-swapping, and stolen API keys to bypass security measures like multi-factor authentication (MFA). This trend underscores the growing need for robust identity and access management protocols in protecting against aviation cybersecurity threats (CrowdStrike Global Threat Report, 2024).

Highlights from CrowdStrike’s 2024 report;

- Identity-based and social engineering attacks still take center stage.
- Cloud-environment intrusions have increased by 75% from 2022 to 2023.
- Third-party relationships exploitation makes it easier for attackers to hit hundreds of targets.

- CrowdStrike added 34 new threat actors in 2023.
- Attackers are compromising networks at a faster rate.
- Attackers are targeting periphery networks.

Another key insight from CrowdStrike's findings is the increased targeting of peripheral networks and supply chains, where attackers exploit vulnerabilities in outdated or unmonitored systems. This tactic enables them to compromise a single-entry point to access multiple interconnected networks, which is particularly concerning for the aviation industry given its reliance on extensive and often interconnected technological infrastructure

CrowdStrike's Role in Mitigating Cybersecurity Threats

Threat Intelligence: CrowdStrike provides advanced threat intelligence to detect emerging threats targeting airport systems. Their Global Threat Reports offer insights into the tactics, techniques, and procedures (TTPs) used by cybercriminals and nation-state actors targeting critical infrastructure.

Endpoint Protection with Falcon Platform: CrowdStrike's Falcon platform offers endpoint protection that detects and prevents threats across devices connected to the airport network. Its cloud-native architecture is suitable for scalable and dynamic airport environments.

Incident Response and Threat Hunting: CrowdStrike's incident response teams help airports quickly contain and mitigate the impact of cyberattacks, reducing downtime. Their proactive threat-hunting capabilities identify potential vulnerabilities before they are exploited.

Case Studies and Real-World Examples

Network disruptions that result in data breaches or operational failures can lead to non-compliance with aviation regulations and standards. This can result in penalties, fines, and increased scrutiny from regulatory bodies. A notable IT outage at Heathrow Airport led to significant delays and the cancellation of flights. This disruption was reportedly due to a power supply issue affecting the airport's IT systems, Heathrow Airport (2017). A power outage caused by a fire disrupted operations for nearly 11 hours, leading to mass flight cancellations and affecting thousands of passengers, Atlanta Hartsfield-Jackson Airport (2017). A major IT failure caused by a power surge led to the cancellation of over 400 flights, stranding passengers worldwide. The incident highlighted the vulnerabilities of centralized IT systems to single points of failure, British Airways (2017). Multiple US airports experienced DDoS attacks that targeted their websites, disrupting online services and causing operational delays. These incidents underscored the need for robust cybersecurity measures to protect airport networks, US Airports (2022).

Air Traffic Control Disruptions with network issues can affect the communication between pilots and air traffic controllers, potentially leading to safety risks and inefficiencies in managing airspace. Disruptions can force air traffic control to revert to manual systems, slowing down operations and increasing the potential for errors International (ICAO, 2016).

Network disruptions can expose sensitive passenger data, such as personal information, travel itineraries, and payment details, to cybercriminals. Such breaches can lead to identity theft, fraud, and a loss of customer trust. In 2018, Cathay Pacific Airways suffered a data breach affecting 9.4 million passengers due to vulnerabilities in its IT infrastructure.

Discussion and Conclusion

Airport technology network disruptions refer to incidents where the digital systems and infrastructure that support airport operations experience failures, leading to significant operational challenges. These disruptions can stem from a variety of causes, including technical malfunctions, cyberattacks, natural disasters, and human error. The complexity of modern airport operations—ranging from flight scheduling, passenger check-in, baggage handling, air traffic control, and security systems—means that even minor disruptions can have widespread implications.

Disruptions can cause delays in flight operations, resulting in missed connections, increased operational costs, and inconvenience to passengers. In severe cases, entire flights may need to be cancelled if critical systems are offline.

Compromised network systems can lead to breaches in airport security, increasing the risk of unauthorized access, smuggling, and other security threats. Delays, long queues, and missed flights negatively impact passenger satisfaction, which can harm the airport's reputation and reduce future business. The financial impact on airlines and airports can be substantial due to operational disruptions, passenger compensation, and brand damage.

To address these challenges, airports must implement robust cybersecurity measures, ensure regular maintenance and upgrades of their technology infrastructure, and conduct thorough training and awareness programs for staff. Using advanced threat detection systems, like those offered by cybersecurity firms such as CrowdStrike, can help identify and mitigate potential threats before they escalate into major disruptions.

By understanding and addressing the causes and impacts of technology network disruptions, airports can enhance their resilience, ensuring smoother and safer operations in an increasingly digital and interconnected aviation environment.

Airport technology network disruptions present significant risks that extend beyond operational inefficiencies to encompass financial, security, and reputational aspects. To minimize these impacts, airports must invest in robust cybersecurity measures, network resilience, regular system maintenance, and staff training. Preparing for potential disruptions and having comprehensive contingency plans in place are crucial steps in ensuring the smooth and safe operation of modern airports.

Suggestion

To address and mitigate airport technology network disruptions effectively, a multi-layered approach that combines advanced technology, rigorous policies, and staff training is essential.

Airports should have well-defined incident response plans outlining the steps to take in the event of a network disruption. This includes isolating affected systems, notifying relevant authorities, and communicating with stakeholders.

Conduct regular drills to test the effectiveness of the incident response plan. Staff should be trained on their roles during a disruption, ensuring they can act quickly and efficiently.

Invest in Staff Training and Awareness Programs such as, regularly train airport staff on cybersecurity best practices, recognizing phishing attempts and securing sensitive information. Employees should be aware of the latest cyber threats and how to respond to them. Launch awareness campaigns to educate staff about the importance of cybersecurity. This can include posters, newsletters, and workshops focused on specific threats like ransomware or social engineering attacks (Capgemini, 2020).

Participate in information-sharing initiatives with other airports, airlines, and government agencies. Sharing intelligence on emerging threats and vulnerabilities can help develop a coordinated response to cybersecurity challenges.

Ensure compliance with national and international cybersecurity regulations and standards, such as those set by the International Civil Aviation Organization (ICAO, 2018) and the European Union Agency for Cybersecurity (ENISA, 2024). Modernization of Infrastructure with legacy systems often pose a security risk due to outdated software and lack of support.

Airports should invest in upgrading these systems to ensure they are compatible with modern security solutions. If replacement is not feasible, legacy systems should be regularly patched and updated to mitigate vulnerabilities.

By implementing these strategies, airports can significantly reduce the risk of network disruptions, enhance operational resilience, and safeguard against the increasingly sophisticated cyber threats that target critical aviation infrastructure.

References

Capgemini (2020), **Collaborative Decision Making in Aviation**. Capgemini's CDM Implementation. Center of Excellence Aviation.

CrowdStrike (2024), **Global Threat Report**, www.crowdstrike.com/global-threat- report

Electronic Transactions Development Agency: ETDA, (2021). **Cybersecurity, "Malware"** https://www.etda.or.th/th/Useful-Resource/What-Is-Malware.aspx

European Union Agency for Cybersecurity (2024). https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

International Civil Aviation Organization. (2016). **Doc 4444 Air Traffic Management. 16th ed.** International Civil Aviation Organization.

International Civil Aviation Organization. (2018). **Doc 9971 Manual on Collaborative Air Traffic Flow Management (ATFM). 3rd ed.** International Civil Aviation Organization.

Jeeradist, T. (2023). **Using Airport Collaborative Decision Making (A-CDM) Network to Improved Aviation Industry Service Quality.** International Journal of Computer Science & Information Technology (IJCSIT) Vol 15, No 1, February 2023.