

ATI SUBMISSION by GROUP 8D



ICT Ethical Issue

Malaysian Airport's Cyber Disruption a Warning for Asia

Transportation facilities and networks slowly adapt to changes and threats, leaving them vulnerable to agile cyberattackers, as demonstrated by the \$10 million ransomware attack.

Editor's Choice

A US\$10 million ransomware attack on the Kuala Lumpur International Airport (KLIA) in Malaysia resulted in hours — if not days — of disruption, a signal that the nation and the region at large must harden defenses against cyberattacks targeting critical infrastructure.

On March 23, travelers at KLIA reported disruptions with flight information display systems, check-in counters, and other services. While KLIA operator Malaysia Airports Holdings Berhad (MAHB) initially confirmed a cyberattack "affecting certain computer systems," the company claimed that operations were not affected. In a speech two days later, Malaysian Prime Minister Anwar Ibrahim called the disruption "quite heavy" and said that a ransom demand for \$10 million had been refused.

The attack underscores the vulnerability of airports and other transportation networks because they are heavily regulated and often do not focus on cybersecurity, says Aaron Bugal, field CISO for Asia Pacific and Japan (APJ) at cybersecurity firm Sophos.

"Critical infrastructure, such as airports, have long-tail regulation and governing bodies that have not responded well to quick-timed changes needed to stay secure and ahead of the cybercriminals," he says. "With this public knowledge and the sometimes glacial pace [at which] critical infrastructure organizations adapt to cyber requirements, [they are] an attractive target given their high impact if an attack is successful."

Issue: Ransomware

Source: <https://www.darkreading.com/cyberattacks-data-breaches/malaysian-airport-cyber-disruption-warning-asia>

Brief Explanation:

On March 23rd, Kuala Lumpur International Airport (KLIA) experienced cyberattack which heavily disrupted their critical information and database systems. Individuals behind this attack demanded a ransom of USD10 Million, which were firmly refused by the Malaysian Prime Minister, Dato' Seri Anwar Ibrahim. This incident highlights a severe cybersecurity threat in critical country's infrastructure such as transportation. This unethical ransomware attacks can cause financial loses, operational shutdowns, and breaches of sensitive data, and it is highly imperative for a robust defense mechanism to be quickly implemented to protect important and sensitive digital infrastructure from such incidents.

General Ethical Issue



Environmental pollution in residential area

This image shows severe environmental pollution where trash and plastic waste are improperly discarded near residential area. This reflects a lack of environmental ethics and social responsibility which could potentially harm human health and local water ecosystem due to unsanitary living conditions.



Lack of responsibility in a Restaurant

This image highlights food waste and a lack of responsibility in a public restaurant. The previous customers left behind excessive leftovers and did not clean up after themselves, demonstrating a disregard for ethical dining etiquette. Ethically, individuals should only order what they can consume and make an effort to keep the dining area tidy and clean. This not only reduces food waste, but also helps lighten the workload of restaurant staff, promoting a more respectful and considerate dining environment.