DHG | IT advisory

AIRPORT CYBERSECURITY

WHY CHOOSE DHG?

DHG's IT Advisory group is experienced with cybersecurity challenges that are unique to the aviation industry and have developed a comprehensive set of services designed to help our clients address cybersecurity risk:

+ Cybersecurity Risk Assessments
+ Network Security Assessments and Penetration Testing
+ Security Awareness Testing and Social Engineering Assessments
+ PCI Compliance Assessments
+ Data Breach Incident Response Forensic Investigations

airport cybersecurity challenges and our capabilities

Designated as critical infrastructure by the federal government, airports are responsible for maintaining a wide variety of data, including credit card information, personally identifiable information (PII) of employees and contractors, airport access control data, and sensitive information about the airport's infrastructure. The lack of a mandatory cybersecurity framework in the aviation industry leaves commercial airports without a common strategy for addressing the increasing threat of a cybersecurity breach. DHG has identified several key challenges that airports face:

Board visibility **Lack of data control** **Lack of threat control** **Ongoing security assessment**

BOARD VISIBILITY

Airport boards of directors and executive leaders often lack visibility into the airport's cybersecurity efforts. Cybersecurity risk management must be driven by the most senior leadership to ensure that resource investment is prioritized, addressing the most critical vulnerabilities that could expose the airport's highly sensitive data.

DHG performs cybersecurity risk assessment services to assist boards and management understand where the airport's most critical vulnerabilities lie.

LACK OF DATA CONTROL

Many airports struggle to understand where their critical data resides. Mobile devices and third party cloud hosting services introduce new challenges around data control and security that airport IT group's overlook as part of their data governance plans.

DHG helps airport IT leadership understand the controls around data at rest, data in motion, and data hosted by third party providers.

LACK OF THREAT AWARENESS

Today's cyber attackers are taking advantage of the weakest link in the technology chain: the end users. Sophisticated and targeted email or phone phishing campaigns are effective at deceiving users that results in access to sensitive systems or data. Small and medium sized airports often overlook the importance of fostering and maintaining a culture of security awareness that is effective in combating these dangerous social engineering attacks.

DHG conducts comprehensive cybersecurity awareness assessment services that include awareness policy development, awareness training content and sessions, and social engineering testing.

ONGOING SECURITY ASSESSMENT

Security is an ongoing process that requires continuous evaluation of the airport's threat environment and current cybersecurity posture. Lean IT resources and alternate business priorities often prevent airports from focusing on cybersecurity as a key business driver.

DHG assists airports with maintaining an effective cybersecurity program with multiple services that include technical network security assessments, compliance assessments, and forensic investigations.