International Civil Aviation Organization

WORKING PAPER

A41-WP/231[1]
EX/104
2/8/22

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

CYBERSECURITY CULTURE STRATEGY

(Presented by Saudi Arabia on behalf of the Arab Civil Aviation Organization (ACAO) States[2])

EXECUTIVE SUMMARY

Cyber-attacks are constantly on the rise across the civil aviation sector, which, in turn, impacts aerodromes, airlines, air traffic and also passengers. The best method to minimize cyber risks is to develop a cybersecurity culture strategy designed to enhance personnel capacity, promote cybersecurity objectives and protect organizations against internal and external cyber threats. The cybersecurity culture strategy is positioned to play a critical role in complying with cybersecurity requirements and fostering cooperation on the organizational, national and international levels. A cybersecurity culture strategy should address all personnel of any organization, as it seeks to establish and maintain a cybersecurity culture to support people, technologies and cybersecurity operations.

Action: The Assembly is invited to:

a) urge Member States to adopt a cybersecurity culture strategy in civil aviation in light of the significant increase in cyber-attacks around the world; and
b) call on ICAO to develop a Cybersecurity awareness programme designed for civil aviation personnel, in parallel with the Aviation Security Culture programme.

Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective
Financial implications:	
References:	

[1] *Arabic version provided by Saudi Arabia.*

[2] *Member States of the Arab Civil Aviation Organization (ACAO): Algeria, Bahrain, Comoros, Djibouti, Egypt, Iraq, Jordan, Kuwait, Lebanon, Libya, Mauritania, Morocco, Oman, Palestine, Qatar, Saudi Arabia, Somalia, Sudan, Syrian Arab Republic, Tunisia, United Arab Emirates, and Yemen.*

1. INTRODUCTION

1.1 Human error was cited as the leading cause of Cybersecurity attacks and breaches in 2021, suggesting that personnel are the weakest link in the Cybersecurity chain. In addition, cybercriminals have launched attacks that target system users to exploit their vulnerabilities. Accordingly, organizations must develop Cybersecurity culture strategies to ensure that their staff properly deal with a vast array of cyber threats that target them or their employment positions. As such, they become their organizations' first line of defence.

1.2 People, processes and technologies constitute Cybersecurity's three main pillars. The three pillars fundamentally depend on a strong Cybersecurity culture, as technology, without adequately trained staff, will create vulnerabilities. Processes in themselves are also ineffective unless they are correctly implemented by staff.

1.3 Human error is not only limited to users clicking on suspicious links or downloading malware. The most significant risk comes from underqualified system developers committing a mistake in configuring or setting up a critical system or failing to follow change management procedures while introducing changes to a system, thereby exposing the overall technical infrastructure to external cyber threats.

1.4 All staff must be cognizant of their roles and responsibilities in applying the organization's Cybersecurity programme. They must also understand their obligations under the cybersecurity policy and any national penal code covering cyber activities.

1.5 Senior management and board directors play a crucial role in promoting Cybersecurity requirements and addressing cyber risks. As such, they need to be aware of Cybersecurity's importance and deal with cyber risks as organizational-level ones.

2. CYBERSECURITY CULTURE

2.1 A Cybersecurity culture promotes information sharing among Member States to proactively identify and address cyber vulnerabilities and threats.

2.2 Effective change begins with Cybersecurity awareness and training. Organizations should therefore take additional steps to effect behavioural changes by adopting a Cybersecurity culture.

2.3 A Cybersecurity culture comprises the following three steps:

a) *identification of strategic objectives:* Identifying a Cybersecurity culture's objectives is the first step in the process. Such objectives may include, *inter alia*, ensuring that personnel fully understand Cybersecurity risks for the organization and are cognizant of their respective roles and responsibilities; as well as enhancing Cybersecurity knowledge and competencies;

b) *assessment of the existing situation*: The objective is to assess the existing culture at the organizational and individual levels. The organizational level reflects the organization's governance and promotion of appropriate behaviours. This may include policies and procedures, acceptable usage policy, roles and responsibilities, awareness and training,

organizational structure, cybersecurity structures, incident reporting and Cybersecurity committee documentation. On the other hand, the individual level investigates staff Cybersecurity awareness through learning platforms or cyber-attack simulations. In the absence of the required technologies, a survey may be developed and disseminated to gather the necessary information.

c) *development of the programme:* The final step is to map out the gap between the current and desired situations and set up the programme to realize the previously identified strategic objectives.

— END—