GACA
الهيئة العامة للطيران المدني
General Authority of Civil Aviation

VISION رؤية 2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA

Cybersecurity in civil aviation

General Authority of Civil Aviation - Aviation Security

Index

Introduction

The senior leadership in the Kingdom of Saudi Arabia has been concerned with cybersecurity and issued several decisions, the most important of which are:

1. Establishing a cybersecurity authority, which is the legislative and supervisory for cybersecurity in government agencies, companies and their affiliated entities.
2. Separating cybersecurity from the information technology sector in all government agencies as well as companies and affiliated entities to prevent conflict of interests, and they are directly linked to the primary official in the Organization.

Responsibility of government, private, and other agencies towards cybersecurity

National Cybersecurity Authority - (NCA)

Enhancing the Kingdom’s cybersecurity requires the cooperation of all parties to work in an integrated national system to face cyber risks and reducing the impact. Therefore, the National Cybersecurity Authority considers each party, whether public or private, as an essential partner to achieve the goals for which the Authority was established for. Also, the authority has confirmed that all authorities in the Kingdom belong to it are responsible towards its cybersecurity and Authority Policies can not exempt those Authorities from protecting their data.

Responsibility of government, private, and other agencies towards cybersecurity

National Cybersecurity Authority - (NCA)

The senior leadership in the Kingdom of Saudi Arabia has announce that:

“all government agencies must raise the level of their cybersecurity to protect their cyber networks, systems and data, and abide by the policies, frameworks, standards, controls and guidelines issued by the National Cyber Security Authority in this regard.”

Responsibility of government, private, and other agencies towards cybersecurity

National Cybersecurity Authority - (NCA)

According to the National Cybersecurity Authority - (NCA) , all relevant authorities are obligated to the following:

1. Enabling the authority to direct its powers and fully implement its tasks.
2. Inform the Authority - immediately - of any actual or potential danger, threat or breach of cybersecurity.
3. Implement policies, governance mechanisms and frameworks, and apply the standards and controls approved by the Authority.
4. Full cooperation with the authority when it performs any investigation, audit or evaluation of cybersecurity
5. Providing the Authority with the documents, information, data and reports necessary to carry out its functions and tasks, and enabling it to examine the devices, networks, systems and software of those entities.

Cybersecurity in civil aviation

GACA
الهيئة العامة للطيران المدني
General Authority of Civil Aviation

Cybersecurity in civil aviation

The General Authority of Civil Aviation in the Kingdom of Saudi Arabia has taken several measures to ensure that the civil aviation entities, including operators, airlines, and others, comply with cybersecurity controls, including:

1. Generalization basic cybersecurity controls issued by the National Cybersecurity Authority to all civil aviation entities.
2. Generalization controls for sensitive systems issued by the National Cybersecurity Authority to all civil aviation entities.
3. Generalization controls for remote work issued by the National Cybersecurity Authority to all civil aviation entities.
4. Issuing cybersecurity controls for security devices and systems and circulating them to all civil aviation entities.
5. Follow up the commitment of the civil aviation authorities to all the mentioned controls, analyze the gaps, and follow up the corrective measures to reach full compliance.
6. Providing cyber awareness programs for the authority's employees and airport employees, and a cyber awareness program for leaders has been prepared and presented.

Essential Controls for Cybersecurity - ECC

The National Cyber Security Authority has developed the basic cyber security controls that aim to provide the minimum basic requirements for cyber security based on best practices and standards to reduce cyber risks on the information and technical assets of the parties from internal and external threats.

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Essential controls for cybersecurity

The Essential controls for cyber security consist of 114 basic controls, divided into five main components:

- Cybersecurity governance
- Enhanced cybersecurity
- Cybersecurity resilience
- Cybersecurity related to third parties and cloud computing
- Cybersecurity for industrial control system

Essential cybersecurity controls are mandatory. All parties, within the scope of these controls, must implement what achieves a permanent and continuous commitment to these controls.

Cybersecurity controls for sensitive systems

The National Cybersecurity Authority has developed cyber security controls for sensitive systems. These controls aim to support basic cybersecurity controls in providing minimum cybersecurity requirements for sensitive systems based on best practices and standards; To meet the current security needs and raise the readiness of the entities within the scope of these controls so that they can protect their sensitive systems and prevent unauthorized access to them, which results in costly risks and losses at the national level.

Controls Cybersecurity Systems Critical - CCSC

Cybersecurity controls for sensitive systems consist of 32 primary officers and 73 sub-officers, divided into four main components:

1. Cybersecurity Governance.
2. Enhanced cybersecurity.
3. cyber security resilience.
4. Cybersecurity related to third parties and cloud computing.

Cybersecurity controls for sensitive systems are considered mandatory controls, if one of the criteria for determining sensitive systems is achieved, as all parties within the scope of these controls must implement what achieves permanent and continuous commitment to these controls.

Cybersecurity Controls for Remote Work

Based on the objectives of the strategy of the National Cybersecurity Authority and in continuation of its role in organizing and strengthening the protection of the Kingdom’s cyberspace, the National Cybersecurity Authority has developed cybersecurity controls for remote work, after studying several international standards, frameworks, controls and practices for cybersecurity. The document aims to contribute to raising the level of cybersecurity at the national level by enabling the entity to perform its work remotely in a safe manner and adapt to changes in the business environment and remote work systems. In addition to enhancing cybersecurity capabilities and resilience against cyber threats when remote work is enabled. These controls are an extension of the basic cybersecurity controls.

Cybersecurity controls for security systems and equipment

The General Authority of Civil Aviation, represented by the General Department of Cybersecurity, has issued cyber security controls for security systems and equipment in accordance with the legislation of the National Cybersecurity Authority.

Cybersecurity controls for security systems and equipment

The purpose of these controls is to provide cybersecurity requirements based on best practices and standards related to the security systems and equipment of the General Authority of Civil Aviation at its domestic and international airports and its affiliates in order to reduce cyber risks and protect them from internal and external threats by focusing on the basic objectives of protection, namely: confidentiality of information, safety, and availability.

These controls aim to comply with the cyber security requirements issued by the National Cybersecurity Authority and the relevant legislative and regulatory requirements.

Cybersecurity Awareness

GACA
الهيئة العامة للطيران المدني
General Authority of Civil Aviation

Steps to implement the training program

- Needs assessment
- Gap analysis
- Setting goals

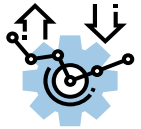
STEP 1

STEP 2

- Develop a training strategy
- Develop a training plan
- Task scheduler

- **Apply for training**
- **Register the Applicant**

STEP 3



STEP 4

- **Final Evaluation**

incomplete Pending Complete

General objectives of the program

- Raising the level of security awareness of the targets.
- Measuring the awareness of the employees of the General Authority of Civil Aviation.
- Identification of potential information security risks and threats.
- Introducing the laws and regulations related to information crimes.
- Dealing with information security incidents and ways to report them

Training Methodology

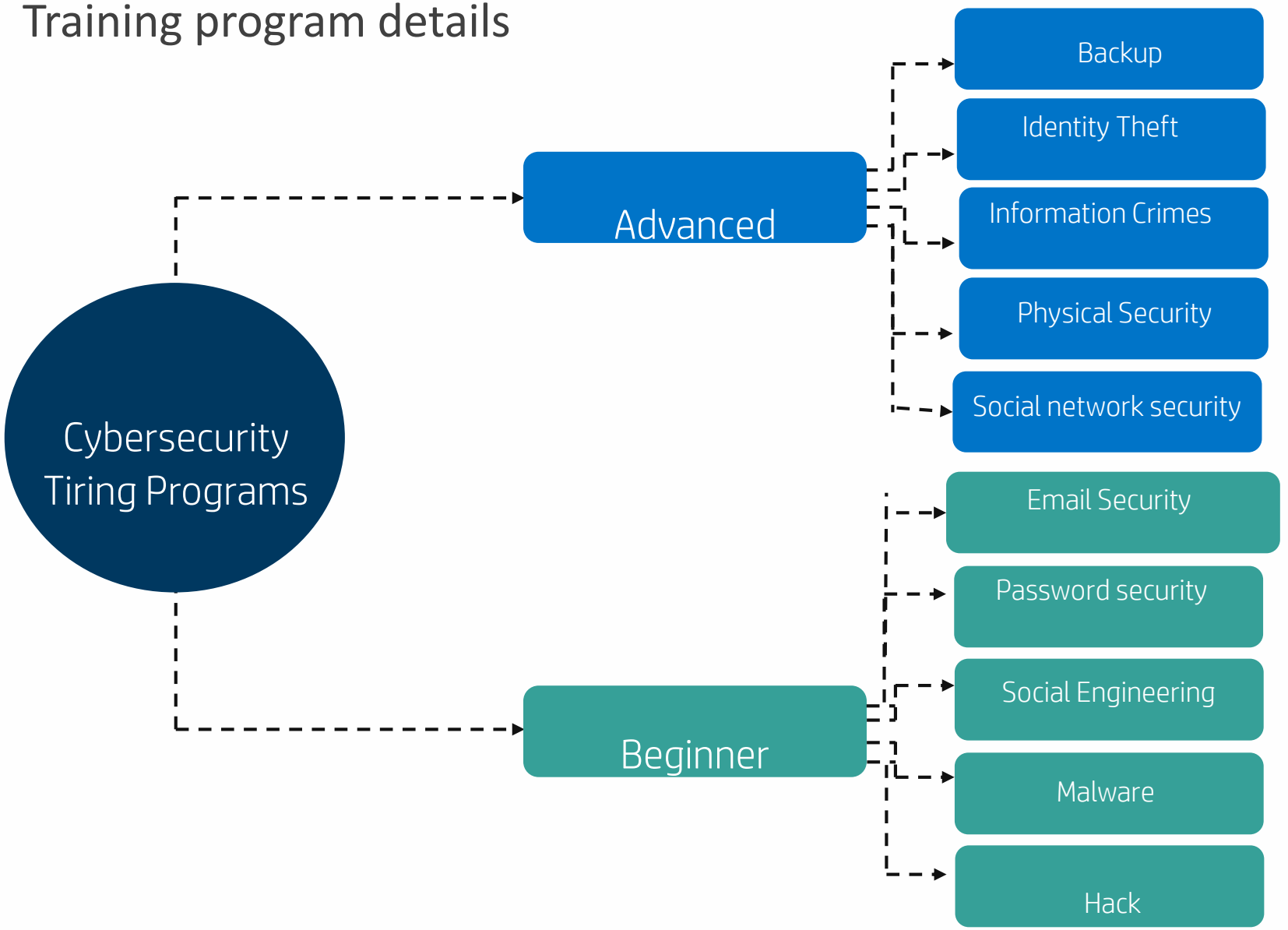
A self-learning experience has been provided to each employee, which develops the knowledge and scientific personality of the authority's cadres. And motivate everyone who seeks answers, as the employee can ask a set of questions about various topics in information security related to the organization and his personal culture.

Training program methodology

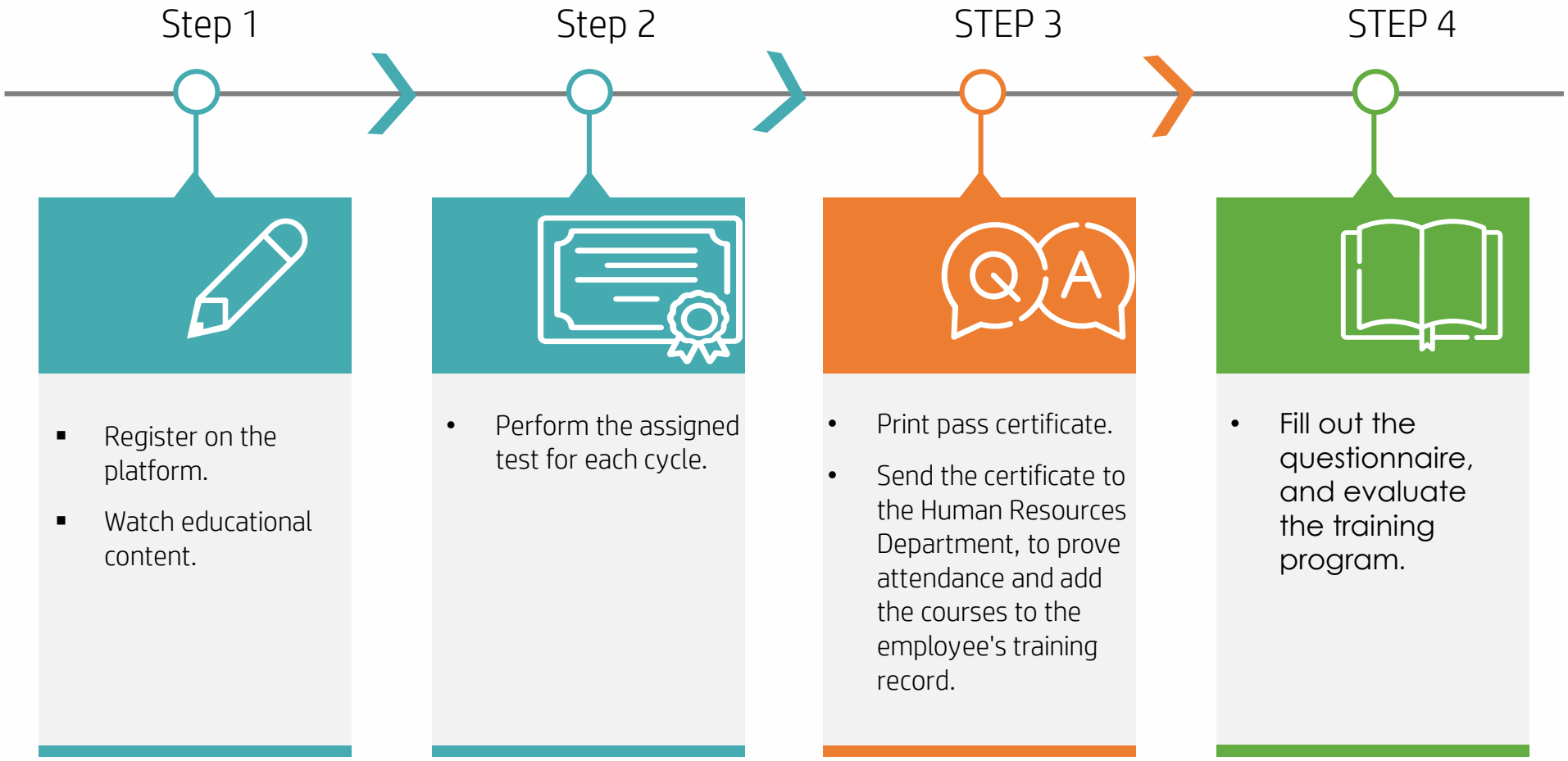
The Roam platform has been approved to provide the training program (Basics of Cybersecurity Beginner and Advanced), which is provided by the Center of Excellence for Information Security at King Saud University.

It is a platform that contains video clips in addition to an electronic test to ensure that the employee understands when passing it, in addition to many methods and accessories that complement the dissemination of awareness.

Training program details



Training steps and passing certificate



- Register on the platform.
- Watch educational content.

- Perform the assigned test for each cycle.

- Print pass certificate.
- Send the certificate to the Human Resources Department, to prove attendance and add the courses to the employee's training record.

- Fill out the questionnaire, and evaluate the training program.

Awareness Certificate

Center of Excellence for Information Security

Awareness Certificate is an approved certificate that an organization obtains when it educates at least 60% of its employees as a whole, or 75% of the employees of one of its departments.

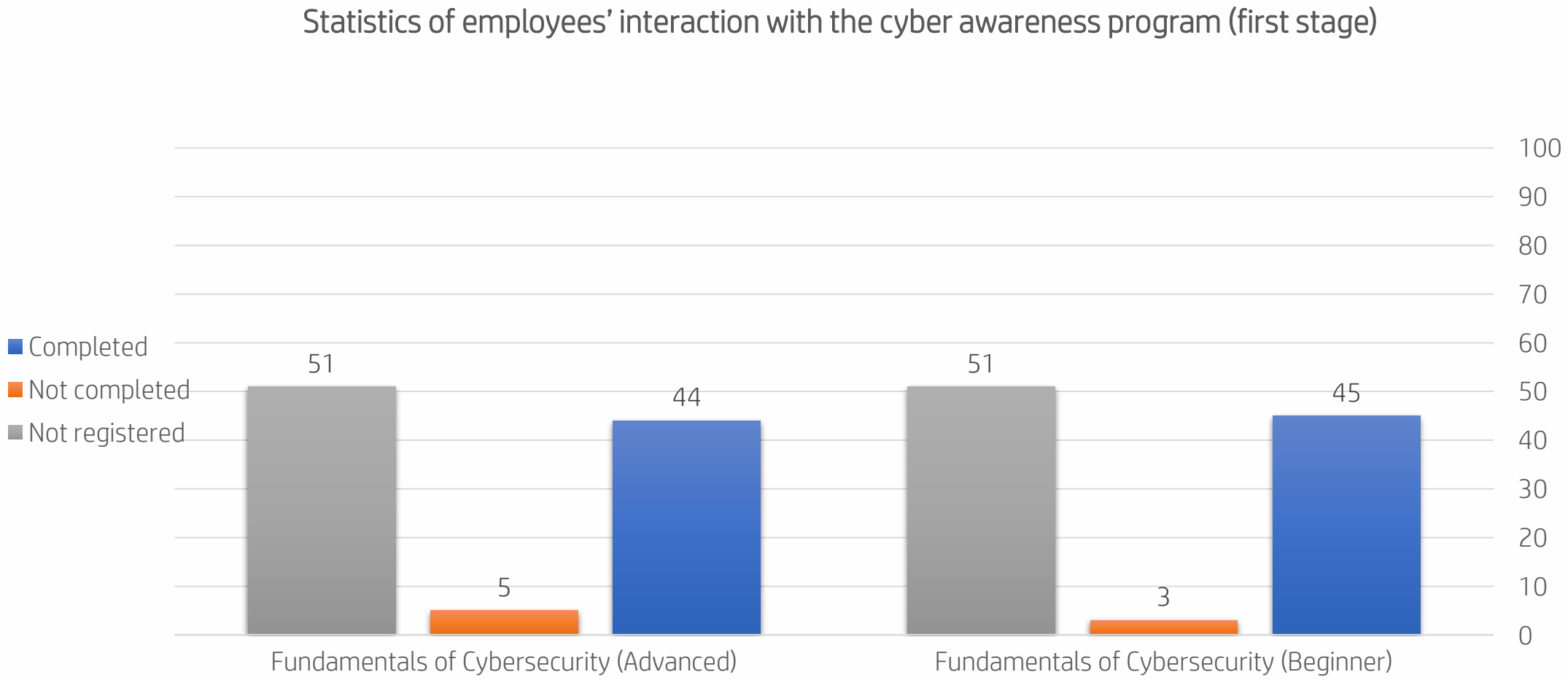
شـهـادة واعــي

Launching the training program

The first phase: from November to the end of December 2020The first phase

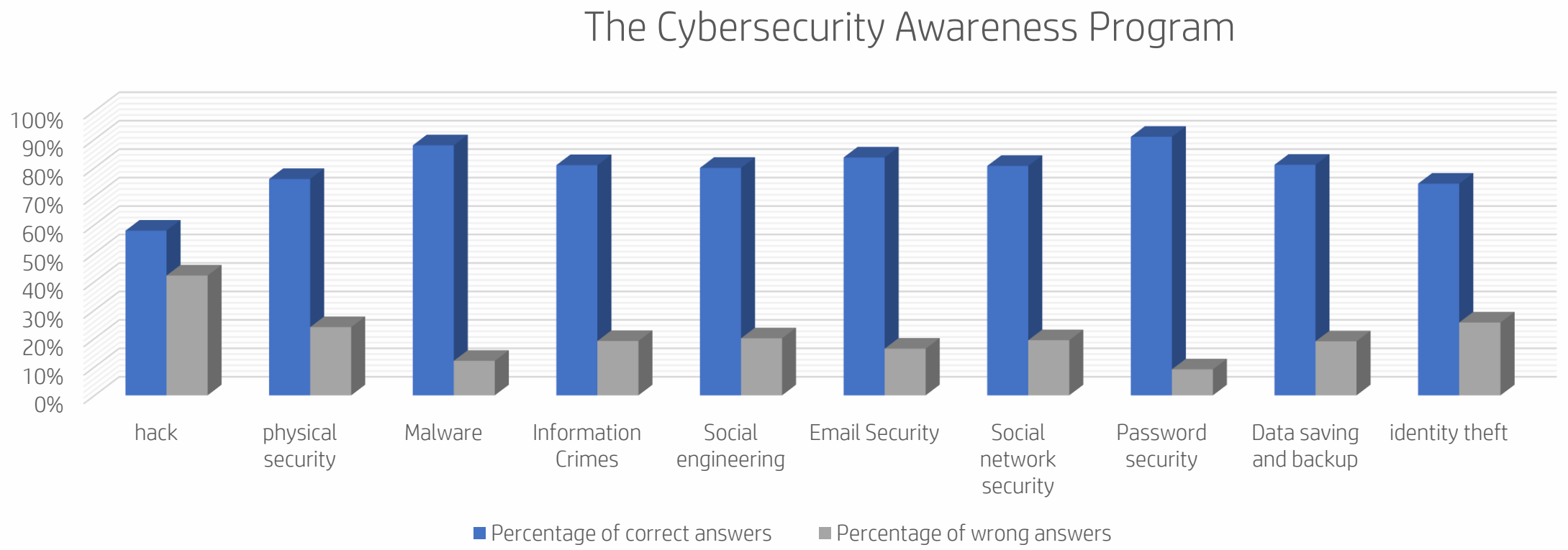
- The first awareness campaign was launched, targeting all employees of the General Authority of Civil Aviation, without exception.
- They were directed to log in to the platform, complete the training program and perform the test, and attach a copy of the program's completion certificate, before the end of the Gregorian year 2020.
- This campaign aims to measure the employees' awareness of the importance of information security, and to interact with this campaign in all seriousness.

Launching the training program



Training Program Results

The test questions are categorized into three levels: easy, medium, and difficult



Training Program

The second phase: 2021

- The second awareness campaign was launched.
- The second campaign targets those who did not complete the training program, and the president's assistants to the sectors were notified of the names of the late employees.
- The deadline is set at the end of February; to complete the training program.

Cybersecurity Awareness Result

End of the second phase: February 2021

The target has been achieved

Awareness of 75% of the staff

Results of employee evaluation of the training program

Reading the program outputs: opinions, evaluations and suggestions

- Comprehensiveness of the training program elements as an introduction to cybersecurity
- Positively interacted with digital content
- Some employees want to enroll in non-compulsory cybersecurity programs
- The desire of some employees who are not specialized in cybersecurity to enroll in specialized programs in the field of cybersecurity

شكـــراً لكـــم

Thank You

GACA®
الهيئـــة العامـة للطيران المدني
General Authority of Civil Aviation

KSAGACA | gaca.gov.sa
8001168888