THE VALUE OF PERFORMANCE

NORTHROP GRUMMAN

Park Air V5 Training

Cybersecurity for ATM Professionals

Introduction

Air Traffic Management communications systems are becoming more digital and more interconnected. The introduction of Voice over IP, increased use of data-communication and a shift to increased connectivity of all elements in the network can bring great benefits to both users and maintainers of equipment, but can also introduce new risks.

This set of courses has been specifically designed by Park Air to introduce ATM professionals - managers, supervisors and engineers - to the fundamentals of Cybersecurity as they apply to an ATC communications network. Bringing together general best practices from the Centre for Internet Security (CIS) with Park Air's deep knowledge of the ATM industry, the courses give professionals who may not have an IT background a set of tools and frameworks with which to assess cybersecurity risk and make informed decisions on steps to mitigate this.

The training modules are described on the following pages.

Table of contents

1 Cybersecurity Overview - The Threat Landscape (V5-O-CYBERTHREAT)

Introduction

This module defines cybersecurity, explains the various threats and how they can damage organisations.

Target audience

- ATC managers and supervisors
- ATC engineers and technicians.

Prerequisite

- None.

Content

- Definition of cybersecurity
- Understanding of cyber threats
- Introduction of cyber attacks
- Case studies.

2 Cybersecurity Overview - Frameworks and Guidelines (V5-O-CYBERFRAMEWORKS)

Introduction

This module introduces the cybersecurity frameworks and guidelines available, explaining their history and how they relate to each other.

Target audience

- ATC managers and supervisors
- ATC engineers and technicians.

Prerequisite

- Cybersecurity Overview - The Threat Landscape (V5-O-CYBERTHREAT).

Content

- Overview of cybersecurity frameworks and guidelines
- Legislation, standards and requirements
- Describe how frameworks and guidelines develop
- Introduction to the NIST Cybersecurity Framework
- Introduction to the CIS Top 20.

3 Cybersecurity Overview - Foundational CIS CSC (V5-O-CYBERFCISCSC)

Introduction

This module introduces the requirements, risks and solutions of the Centre for Internet Security's Foundational Cyber Hygiene - the top five Critical Security Controls.

Target audience

- ATC managers and supervisors
- ATC maintenance engineers and technicians.

Prerequisite

- Cybersecurity Overview - The Threat Landscape (V5-O-CYBERTHREAT)
- Cybersecurity Overview - Frameworks and Guidelines (V5-O-CYBERFRAMEWORKS).

Content

- Introduction to Foundational Cyber Hygiene
- Step-by-step guide to the requirements, risks and solutions of the CIS CSC top five.

4 Cybersecurity Overview - Advanced CIS CSC (V5-O-CYBERACISCSC)

Introduction

This module introduces the requirements, risks and solutions of the Centre for Internet Security's Advanced Critical Security Controls.

Target audience

- ATC managers and supervisors
- ATC maintenance engineers and technicians.

Prerequisite

- Cybersecurity Overview - The Threat Landscape (V5-O-CYBERTHREAT)
- Cybersecurity Overview - Frameworks and Guidelines (V5-O-CYBERFRAMEWORKS)
- Cybersecurity Overview - Foundational CIS CSC (V5-O-CYBERFCISCSC).

Content

- Introduction to Advanced Critical Security Controls
- Step-by-step guide to the requirements, risks and solutions of the Advanced CIS CSC.

5 Cybersecurity Overview - Risk Management (V5-O-CYBERRISKMGMT)

Introduction

This module introduces risk management and describes how to identify and reduce risks in a system. A short analysis of risk identification and mitigation using ATM equipment is included.

Target audience

- ATC managers and supervisors
- ATC maintenance engineers and technicians.

Prerequisite

- Cybersecurity Overview - The Threat Landscape (V5-O-CYBERTHREAT)
- Cybersecurity Overview - Frameworks and Guidelines (V5-O-CYBERFRAMEWORKS)
- Cybersecurity Overview - Foundational CIS CSC (V5-O-CYBERFCISCSC)
- Cybersecurity Overview - Advanced CIS CSC (V5-O-CYBERACISCSC).

Content

- Introduction to risk management
- Using physical and logical approaches to determine risks
- The layered security model
- Examples of hardening ATM equipment.

Note:

The information and specifications provided in this document represent the minimum performance of Park Air Systems' equipment. Park Air Systems reserves the right to change the specifications of its equipment from time to time in its discretion without any notice. It is the customer's responsibility to request and obtain the latest applicable specifications from Park Air before placing orders for Park Air Systems' equipment. Neither this document, nor any of the information presented in it, should be regarded as an offer or commitment or a representation on the part of Park Air Systems (or any other person) to enter into a contractual arrangement. For further details please see the Northrop Grumman website.

For more information, please contact:


Northrop Grumman, Park Air Systems Ltd., Northfields, Market Deeping, Peterborough, PE6 8UE, United Kingdom


44 (0) 17 78 34 54 34


sales@parkairsystems.com


www.northropgrummaninternational.com

22/2018