CYBERRISK INTERNATIONAL

AVIATION SECTOR

CYBER INCIDENT RESPONSE

2 DAY EXECUTIVE BOOTCAMP

Executive Strategies in Planning and Responding to Cyber Attacks

COURSE OVERVIEW

It is no secret that the aviation sector is a particular focus for cyber threat actors. The sector is interdependent and interconnected and any impact on it may have a knock on or contagion effect upon the wider industry. Cybercriminals have developed targeted methodologies and resources in order to compromise what they see as "green field" targets.

Cyber resilience, including incident response, is a leadership issue and those with the responsibility of protecting the aviation sector need to understand how to handle a cyber incident.

CRI has developed a non-technical course specifically for senior executives that wish to understand what is involved in planning for and responding to cyber attacks in the aviation sector.

Delegates of this two-day bootcamp course will learn why the aviation sector has become such a hot target for the cyber threat actors and gain a holistic understanding of the cyber incident response process. The syllabus outlines all the stages involved from prevention to eradication and recovery. Delivered by a highly experienced cyber security expert, referencing real life case studies and outlining practical and pragmatic steps every organisation can take.

WHAT YOU WILL LEARN

MODULE 1
Cyber Threats and the Aviation Sector

+ Understanding Cyber Resilience
+ Cyber Threat Landscape 2020
+ Aviation Sector Interconnected and Interdependent
+ Complex Regulatory Landscape
+ Sector Characteristics
+ Specific Digital Challenges
+ Emerging Threats
+ Developing a Cyber Strategy

MODULE 2
Incident Response Introduction

+ Understanding the Incident Response Process
+ Prevention
+ Planning
+ Preparation
+ Reporting
+ Prepare Information Sheets and Checklists
+ Train the Response Team and Practice the Plan
+ Have the Right Tools
+ Outsource Monitoring and Testing
+ Detection
+ Precursors and Indicators
+ Tools Used to Detect Cyber Attacks
+ Situational Awareness Categorisation
+ Documentation
+ IR in a Nutshell

MODULE 3
Elevate and Communicate

+ Preparing a Team for a Cyber Attack
+ Identify Key Actors and their Roles
+ Key Responsibilities of the CSIRT
+ CSIRT Roles
+ CSIRT Models
+ The Cyber Crisis Communication Plan
+ Role and Elements of the Crisis Communication Plan
+ Communicating with Key External Stakeholders
+ The Media
+ Law Enforcement
+ Regulators
+ Incident Reporting Organisations
+ Impacted External Parties
+ Communicating with Internal Stakeholders
+ Channels of Communication
+ Escalation Strategies
+ Putting it Altogether

MODULE 4
Eradicate and Recover

+ Eradication
+ Recovery
+ Post-Incident Analysis
+ Lessons Learned Meeting
+ Incident Report
+ Complete the Improvement Feedback Loop
+ Empowering the Board with Key Metrics

MODULE 5
TTX - Tabletop Exercise

Workshop: Walk through of a real life cyber attack scenario on an entity from the aviation sector

WHO IS THE COURSE FOR?

- ✓ CISO, Head of IT Security
- ✓ CRO, Head of Risk
- ✓ CIO, CTO and IT Directors
- ✓ Project Managers and BCP Managers
- ✓ IT Managers and Service Managers
- ✓ Mid to Senior IT Administrator and Network Managers
- ✓ Change and Incident Managers
- ✓ Head of Audit & Senior Auditors Information Security Managers
- ✓ Head of Security Legal and Compliance
- ✓ Any Senior Executive with Responsibility for Cyber Risk

CYBERRISK INTERNATIONAL

Please contact us for further details.

Cyber Risk International Ltd.
Unit 1 St. Olaves Centre
Malahide Road
Kinsealy
Co. Dublin

+353 (0)1 905 3260

info@cri.ie

www.cyberrisk.ie